Neue Möglichkeiten von ViPNet VPN 4.x

Anhang zum ViPNet VPN Benutzerhandbuch

infotecs

Ziel und Zweck

Dieses Handbuch beschreibt die Installation und Konfiguration von ViPNet Produkten. Für die neuesten Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere Release Notes lesen – insbesondere, wenn Sie ein Software-Upgrade zu einem höheren Release-Stand durchführen. Die aktuellsten Release Notes sind immer zu finden unter http://www.infotecs.de

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in Ihrem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Der Hersteller haftet nur im Umfang seiner Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen, sowie Änderungen und Release Notes für ViPNet Produkte finden Sie unter http://www.infotecs.de. Der Hersteller übernimmt keine Verantwortung für Datenverlust und Schäden, die durch den unsachgemäßen Betrieb des Produkts entstanden sind.

Copyright

1991–2015 Infotecs GmbH, Berlin

Version: 00121-04 90 06 DEU

Dieses Dokument ist Teil des Softwarepaketes und unterliegt daher denselben Lizenzbestimmungen wie das Softwareprodukt.

Dieses Dokument oder Teile davon dürfen nicht ohne die vorherige schriftliche Zustimmung der Infotecs GmbH verändert, kopiert, weitergegeben etc. werden.

ViPNet ist ein registriertes Warenzeichen des Softwareherstellers Infotecs GmbH.

Marken

Alle genannten Markennamen sind Eigentum der jeweiligen Hersteller.

Wie Sie Infotecs erreichen

Infotecs GmbH

Oberwallstr. 24

10117 Berlin

Deutschland

Tel.: +49 (0) 30 206 43 66 0

Fax: +49 (0) 30 206 43 66 66

WWW: http://www.infotecs.de

E-Mail: support@infotecs.de

Inhalt

Einführung **6**
Über dieses Dokument 6
Zielgruppe 6
Verwendete Konventionen 6
Kontakt 8
FAQ und andere Hilfsinformation 8
Kontakt 8

Neue Möglichkeiten von ViPNet Network Manager **8**
Änderung des Namens der Softwarelösung 8
Geänderte Oberfläche des Programms 9
Lizenzierung 10
Neues Lizenzdatei-Format 10
Import der Lizenzdatei 10
Gesonderte Berücksichtigung von Lizenzen für unterschiedliche Typen von Clients und Coordinatoren 10
Zentralisierte Lizenzverteilung 11
Änderung der Lizenzeinschränkungen für die Testversion von ViPNet VPN 11
Aufhebung der Lizenzeinschränkung für die Anzahl der getunnelten Verbindungen 12
Lizenzierung der Verwendung des Programms ViPNet Business Mail 12
Unterstützung neuer Komponenten und Technologien 13
Neue Modifikationen von ViPNet Coordinator HW/VA 13
Verwendung der Software ViPNet StateWatcher und ViPNet Policy Manager an Clients mit dem Typ ViPNet Client Windows 13
Verwendung des Softwaresystems ViPNet StateWatcher 14
Verwendung des Programms ViPNet Policy Manager 14
Unterstützung der Software ViPNet Client for Mac OS X 14
Unterstützung von ViPNet ThinClient 14
Unterstützung von ViPNet Client for Android 14
Unterstützung von ViPNet Connect 15
Unterstützung der ViPNet Failover Technologie 15
Änderung der Knoteneinstellungen 15
Vereinfachung der Netzwerkknoten-Einstellungen 15
Keine Funktion zur Verwaltung der Berechtigungen 17
Definition der DNS-Serverliste 17

Definition der Netzwerkeinstellungen von ViPNet Coordinator HW/VA 18
Vereinfachte Konfiguration der Firewall für Clients 19
Änderungen in der IPsec-Konfiguration für Netzwerkknoten ViPNet Coordinator HW/VA 19
Konfiguration der Liste der verwalteten Knoten für das ViPNet Policy Manager 19
Erstmaliger Start des Programms ViPNet Network Manager ohne Netzwerk-Erstellung 20
Keine Funktion zum Erstellen des Stammzertifikats 20
Möglichkeit zur Änderung des Benutzerpassworts während beliebiger Sitzung im Programm ViPNet Network Manager 20
Anzeige und Wechsel des Netzwerkknotenadministrator-Passworts 21
Wechsel des Internetzwerk-Masterschlüssels 21
Möglichkeit zum Deaktivieren der Überprüfung der Datenvollständigkeit 22

Neue Möglichkeiten von ViPNet Client und ViPNet Coordinator 23
Installation und Upgrade 23
Installation der ViPNet Software 23
Installation der ViPNet Schlüssel 25
ViPNet Updatesystem 26
Traffic-Schutz 27
Filterung des Traffics 27
Objektgruppen 38
Standardparameter der integrierten Firewall 40
Sicherheitsstufen 41
Antispoofing 42
Konfiguration der Netzwerkadapterparameter 43
Sperre des Computers und IP-Traffics 43
Benachrichtigung über Änderungen der Objektgruppen, Netzwerkfilter oder NAT-Regeln 45
Anbindung an ViPNet Netzwerk 46
Konfiguration der Verbindung des Coordinators zum externen Netzwerk über eine Firewall mit statischem oder dynamischem NAT 46
Konfiguration der Clientverbindung zum ViPNet Netzwerk 47
Verbindung der Clients zum ViPNet Netzwerk über einen TCP-Tunnel 48
Sonstige Änderungen 50
Verwendung des Programms ViPNet Client mit vereinfachter Oberfläche 50
Authentisierungsmodus 51
Wechsel der Programmkonfigurationen nach Zeitplan 52
Änderungen im Programm ViPNet Business Mail 53
Hinzufügen von getunnelten Adressen 56

Ermitteln und Überprüfen von IP-Adressen 57
Logdatei der IP-Pakete 57
Integration mit dem Programm SafeDisk-V 59
Übermitteln von MFTP-Dateien über Mailserver 59
Neue Möglichkeiten im verschlüsselten Chat 60
Änderungen der Benutzeroberfläche 61
Änderungen der Terminologie 63

Einführung

Über dieses Dokument

Zielgruppe

Dieses Dokument wendet sich an technische Fachleute, Partner von Infotecs GmbH und ViPNet Netzwerkadministratoren, die ein Update der Software ViPNet VPN auf die Version 4.x planen.

Verwendete Konventionen

Weiter unten sind Konventionen aufgeführt, die im gegebenen Dokument zur Kennzeichnung wichtiger Informationen verwendet werden.

Tabelle 1. Symbole, die für Anmerkungen benutzt werden

Symbol	Beschreibung
	Achtung! Dieses Symbol weist auf einen Vorgang hin, der für die Daten- oder Systemsicherheit wichtig ist.
	Hinweis. Dieses Symbol weist auf einen Vorgang hin, der es Ihnen ermöglicht, Ihre Arbeit mit dem Programm zu optimieren.
	Tipp. Dieses Symbol weist auf zusätzliche Informationen hin.

Tabelle 2. Notationen, die zur Kennzeichnung von Informationen im Text verwendet werden

Notation	Beschreibung
Name	Namen von Elementen der Benutzeroberfläche. Beispiele: Fensterüberschriften, Feldnamen, Schaltflächen oder Tasten.
Taste+Taste	Tastenkombinationen. Zum Betätigen von Tastenkombinationen sollte zunächst die erste Taste gedrückt und dann, ohne die erste Taste zu lösen, die zweite Taste gedrückt werden.
Menü > **Untermenü** >	Hierarchische Abfolge von Elementen. Beispiele: Menüeinträge oder Bereiche der Navigationsleiste.

Notation	Beschreibung
Befehl	
`Code`	Dateinamen, Pfade, Fragmente von Textdateien und Codeabschnitten oder Befehle, die aus der Befehlszeile ausgeführt werden.

Kontakt

FAQ und andere Hilfsinformation

Informationen über ViPNet-Produkte und Lösungen, gängige Fragen und andere nützliche Hinweise sind auf der Webseite von „InfoTeCS“ zusammengefasst. Unter den aufgeführten Links können Sie zahlreiche Antworten auf mögliche während des Produktbetriebs auftretenden Fragen finden.

- Allgemeine Geschäftsbedingungen http://www.infotecs.de/about/terms.php
- ViPNet-Lösungen im Überblick http://www.infotecs.de/solutions/
- Frequently Asked Questions http://www.infotecs.biz/doc_vipnet/DEU/index.htm#2_11572.htm
- ViPNet-Wissensdatenbank http://www.infotecs.biz/doc_vipnet/DEU/index.htm#1_main.htm

Kontakt

Bei Fragen zur Nutzung von ViPNet-Software sowie möglichen Wünschen und Anregungen nehmen Sie Kontakt mit den Mitarbeitern der Firma „InfoTeCS GmbH“ auf. Für die Lösung aufgetretener Problemfälle wenden Sie sich an den technischen Support.

- E-Mail: support@infotecs.de.
- Anfrage an den technischen Support via Internetseite http://infotecs.de/support/
- Support Hotline +49 (0) 30 206 43 66 22 (Tel.); +49 (0) 30 206 43 66 66 (Fax).

Neue Möglichkeiten von ViPNet Network Manager

Änderung des Namens der Softwarelösung

Der Name des Softwarepakets ViPNet OFFICE wurde auf ViPNet VPN geändert. Zusätzlich wurden die folgenden Anwendungen umbenannt:

- das Programm ViPNet Manager wurde in ViPNet Network Manager umbenannt;

- Die Software ViPNet Security Gateway wurde folgendermaßen umbenannt:
  - die für die Installation auf den Computer bestimmte Version trägt den Namen ViPNet Coordinator HW;
  - die für die Bereitstellung in einer virtuellen Umgebung bestimmte Version trägt den Namen ViPNet Coordinator VA.

Geänderte Oberfläche des Programms

Wegen der Vereinfachung der Vorgehensweise beim Konfigurieren der Netzwerkknoten und einigen Änderungen in anderen Funktionen wurde die Oberfläche des Programms ViPNet Network Manager überarbeitet.

Tabelle 3. Grundlegende Änderungen in der Benutzeroberfläche

Was wurde geändert	Version 3.x	Version 4.x
Registerkarten **Firewall des Clients**, **Benutzerrechte** sowie **IP-Adressen** und **DNS-Namen** der Clients	Vorhanden	Fehlt
Registerkarten **IP-Adressen** und **DNS-Namen** der Coordinatoren	Zwei separate Registerkarten	Zu einer Registerkarte **Zugangsadressen** zusammengeführt
Registerkarte **Netzwerkeinstellungen** für ViPNet Coordinator HW/VA	Fehlt	Vorhanden
Registerkarte **Passwörter** des Bereichs **Eigenes Netzwerk**	Fehlt	Vorhanden
Konfiguration der Speicherung des Passworts auf den Knoten	Registerkarte **Benutzerrechte**	Registerkarte **Schlüssel**
Konfiguration der externen Adressen der Firewalls	Registerkarte **Firewall**	Für Coordinatoren auf der Registerkarte **Zugangsadressen**, für Clients wird diese Funktion nicht durchgeführt
Auswahl des VPN-Servers für die Clients	Registerkarte IP-Adressen	Wird nicht durchgeführt
Konfiguration der Verwendung von ViPNet Business Mail	Fehlt	Registerkarte **Schlüssel**

Was wurde geändert	Version 3.x	Version 4.x
Konfiguration der maximalen Anzahl an getunnelten Verbindungen	Registerkarte **Tunnel**	Wird nicht durchgeführt
Netzwerkaufbau-Assistent		Seiten mit den Verbindungseinstellungen von Coordinatoren wurden geändert

Lizenzierung

Neues Lizenzdatei-Format

Im Lizenzsystem wurde aus Optimierungszwecken ein neues Format der Lizenzdatei eingeführt. Nun besitzt die Lizenzdatei die Erweiterung `.itcslic`. Ältere Dateien mit der Erweiterung `.reg` werden ebenfalls unterstützt.

Import der Lizenzdatei

Zur Aktualisierung der Netzwerklizenz musste bis jetzt die Datei `infotecs.reg` in den Installationsordner von ViPNet Network Manager kopiert und das Programm neu gestartet werden. Nun kann die Lizenzdatei unmittelbar im Programmfenster von ViPNet Network Manager importiert werden. Wählen Sie im Menü **Hilfe** den Befehl **Lizenzdatei laden**.

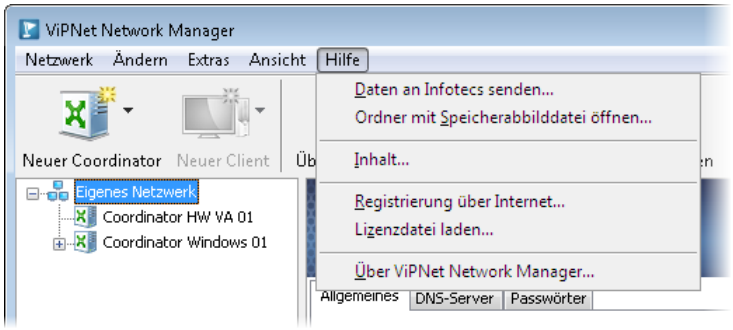

Abbildung 1. Import der Lizenzdatei

Gesonderte Berücksichtigung von Lizenzen für unterschiedliche Typen von Clients und Coordinatoren

Beim Hinzufügen von Clients und Coordinatoren zum Netzwerk wurde bisher sowohl die Gesamtanzahl an verfügbaren Lizenzen für Clients und Coordinatoren als auch die Anzahl an freien Lizenzen für

bestimmte Typen von Clients und Coordinatoren verringert. Beispiel: beim Erstellen des Coordinators ViPNet Coordinator HW/VA wurde sowohl die Anzahl an freien Lizenzen für alle Coordinatoren (Gesamtanzahl) als auch die Anzahl der Lizenzen für Coordinatoren vom Typ ViPNet Coordinator HW/VA herabgesetzt. Nun wird die Berechnung der Anzahl an freien Lizenzen für Clients und Coordinatoren für jeden Typ getrennt durchgeführt.

Zentralisierte Lizenzverteilung

Zusätzliche ViPNet Software und Funktionen konnten zuvor separat für jeden Knoten im Programm ViPNet Network Manager in der Registerkarte **Schlüssel** festgelegt werden. Jetzt können die Lizenzeinschränkungen für die Verwendung von zusätzlichen ViPNet Komponenten zentralisiert für alle benötigten Knoten im Bereich **Eigenes Netzwerk** in der Registerkarte **Allgemeines** verteilt werden.

Abbildung 2. Lizenzeinschränkungen für zusätzliche ViPNet Komponenten

Änderung der Lizenzeinschränkungen für die Testversion von ViPNet VPN

Die Lizenzeinschränkungen für die Testversion von ViPNet VPN wurden gelockert. Nun können mit Hilfe einer nicht registrierten Version von ViPNet Network Manager alle Typen von Coordinatoren und Clients erstellt werden. Ebenso ist der Einsatz der Programme ViPNet Policy Manager, ViPNet Business Mail, ViPNet SafeDisk-V, ViPNet Connect und ViPNet Failover möglich. Mit Hilfe der Softwarelösung ViPNet StateWatcher können außerdem bis zu zehn Knoten überwacht werden.

Aufhebung der Lizenzeinschränkung für die Anzahl der getunnelten Verbindungen

Früher konnte im Programm ViPNet Network Manager nur eine bestimmte Anzahl der Tunnel definiert werden, die von der Lizenz für ViPNet VPN begrenzt war. Nun wurde die Lizenzeinschränkung für die Anzahl der Tunnel aufgehoben. Beim Update von ViPNet VPN einer früheren Version wird die vorhandene Begrenzung für die Anzahl an gleichzeitig getunnelten Knoten für alle Coordinatoren gelöscht.

Lizenzierung der Verwendung des Programms ViPNet Business Mail

Im Programm ViPNet Network Manager wurde eine Lizenzeinschränkung für die Verwendung des Programms ViPNet Business Mail eingeführt. Bei der Installation der Software ViPNet Client wird das Programm ViPNet Business Mail nun nicht mehr standardmäßig auf den Client installiert. Für die Installation und Verwendung dieses Programms auf den Netzwerkclients sollte im Programm ViPNet Network Manager für alle betroffenen Clients auf der Registerkarte **Schlüssel** das Kontrollkästchen **Business Mail verwenden** aktiviert werden. Dann sollten Schlüsselupdates an die Knoten versendet werden. Anschließend kann das Programm ViPNet Business Mail auf die benötigten Clients installiert werden.

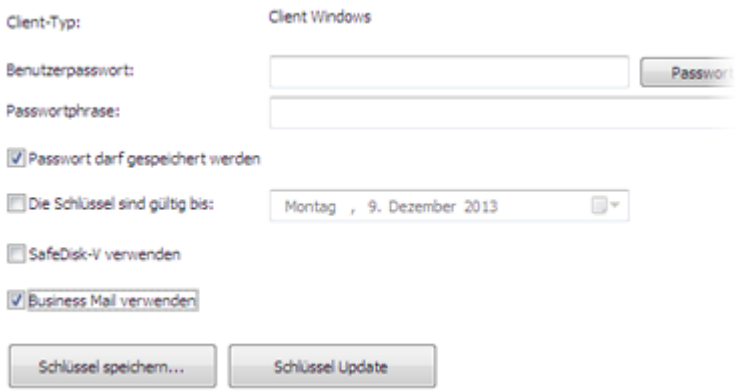

Abbildung 3. Verwendung der Software ViPNet Business Mail erlauben

Unterstützung neuer Komponenten und Technologien

Neue Modifikationen von ViPNet Coordinator HW/VA

Nun können Sie in Ihrem Netz das Softwaresystem ViPNet Coordinator HW1000 und HW2000 sowie Virtual Appliances ViPNet Coordinator VA1000 und VA2000 einsetzen, sofern Sie eine passende Lizenz dafür besitzen.

Alle Ausführungen von ViPNet Coordinator HW und ViPNet Coordinator VA übernehmen die gleichen Aufgaben im Netz. Die grundliegenden Unterschiede zwischen den vorhandenen Modifikationen sind durch die Begrenzungen der Leistungsfähigkeit der Coordinatoren und der Anzahl der unterstützten Netzwerkadapter bedingt.

Bei der Verwendung von ViPNet Coordinator HW und ViPNet Coordinator VA steht Ihnen nun die ViPNet Failover Funktion zur Verfügung, die Sie bei Bedarf aktivieren können. Die ViPNet Failover Technologie ermöglicht es Ihnen, einen fehlertoleranten Cluster aus zwei ViPNet Coordinator HW oder ViPNet Coordinator VA aufzubauen.

Verwendung der Software ViPNet StateWatcher und ViPNet Policy Manager an Clients mit dem Typ ViPNet Client Windows

Früher konnten die Programme ViPNet StateWatcher und ViPNet Policy Manager automatisch auf dem Client verwendet werden, der als Manager-Arbeitsplatz festgelegt war. Nun besteht die Möglichkeit, diese Rollen anderen Clients des ViPNet Netzwerks zuzuweisen (mit Ausnahme der Knoten ViPNet Client Mac OS, ViPNet ThinClient und mobiler Clients).

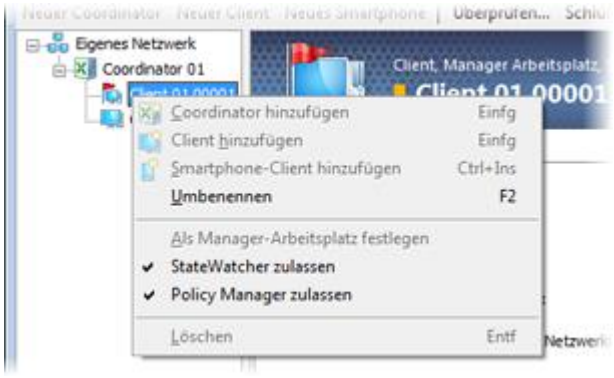

Abbildung 4. Verwendung der Software ViPNet StateWatcher und ViPNet Policy Manager aktivieren

Verwendung des Softwaresystems ViPNet StateWatcher

Im ViPNet VPN-Netzwerk kann nun das Softwaresystem ViPNet StateWatcher verwendet werden. Dieses Softwaresystem dient der Überwachung der Netzwerkknoten mit dem Ziel, Daten über den Status der Knoten zu ermitteln und mögliche Fehler im Betrieb der Knoten aufzudecken. Die Software kann auf beliebegen ViPNet Client für Windows installiert werden.

Verwendung des Programms ViPNet Policy Manager

Es besteht nun die Möglichkeit, die Sicherheitsrichtlinien der Netzwerkknoten, auf denen die Software ViPNet Client und ViPNet Coordinator installiert ist, mit Hilfe des Programms ViPNet Policy Manager zentralisiert zu verwalten. Dieses Programm kann auf beliebegen ViPNet Client für Windows installiert werden.

Unterstützung der Software ViPNet Client for Mac OS X

Vom Programm ViPNet Network Manager wurde zuvor die Software ViPNet Client für Windows unterstützt. Nun besteht die Möglichkeit, die Software ViPNet Client for Mac OS X auf den Netzwerkknoten zu verwenden. Für die Clients dieses Typs werden die Software- und Schlüsselupdates nicht gemeinsam mit den Updates anderer Knoten versendet, sondern vom Netzwerkadministrator separat weitergeleitet. Außerdem können Clients dieses Typs nicht als Manager-Arbeitsplatz eingerichtet werden.

Unterstützung von ViPNet ThinClient

Es kann nun die integrierte Hard- und Softwarelösung ViPNet ThinClient als Netzwerkclient eingesetzt werden. ViPNet ThinClient wird zum Bereitstellen geschützter Benutzer-Arbeitsstationen verwendet und erfüllt die Funktionen eines Terminalclients. Dabei wird die Verschlüsselung und die Filterung des IP-Traffics sichergestellt.

Unterstützung von ViPNet Client for Android

Es besteht nun die Möglichkeit, die Software ViPNet Client Android auf den Clients im ViPNet Netzwerk zu verwenden. Mit Hilfe der Software ViPNet Client Android können Clients zum ViPNet Netzwerk hinzugefügt werden, die unter der Steuerung des Betriebssystems Android arbeiten. Ein Client dieses Typs kann nicht als Manager-Arbeitsplatz festgelegt werden.

Unterstützung von ViPNet Connect

Im Programm ViPNet Network Manager kann jetzt die Verwendung der Software ViPNet Connect auf den Clients ViPNet Client für Windows, ViPNet Client for Android, ViPNet Client für Mac OS X erlaubt werden. Die Benutzer des ViPNet Netzwerkes können mit Hilfe dieses Programms über den geschützten VPN-Kanal einander anrufen. In der ViPNet VPN Testversion wurde auch die Möglichkeit, das Programm ViPNet Connect auf zehn Clients zu verwenden, hinzugefügt.

Unterstützung der ViPNet Failover Technologie

Bei der Verwendung von ViPNet Coordinator HW/VA steht Ihnen nun die ViPNet Failover Funktion zur Verfügung, die Sie bei Bedarf aktivieren können. Die ViPNet Failover Technologie ermöglicht es Ihnen, einen fehlertoleranten Cluster aus zwei ViPNet Coordinator HW oder ViPNet Coordinator VA aufzubauen.

Die Berücksichtigung der Lizenzeinschränkungen für zusätzliche ViPNet Failover Software wird für jede Modifikation von ViPNet Coordinator HW oder ViPNet Coordinator VA einzeln durchgeführt.

Abbildung 5. Lizenzüberprüfung von ViPNet Failover

Änderung der Knoteneinstellungen

Vereinfachung der Netzwerkknoten-Einstellungen

Früher war für die Konfiguration der Netzwerkknoten im Programm ViPNet Network Manager die Ausführung zahlreicher Schritte notwendig, was für den Netzwerkadministrator einige Schwierigkeiten verursachen konnte. Nun wurde die Vorgehensweise bei der Konfiguration der Netzwerkknoten überarbeitet und wesentlich vereinfacht:

- Die Konfiguration der IP-Adressen und DNS-Namen der Coordinatoren sowie die Konfiguration der IP-Adressen und DNS-Namen der Coordinator-Firewall wird nun auf einer Registerkarte **Zugangsadressen** durchgeführt.

- Eine zentralisierte Konfiguration der Firewall der Clients wird nicht mehr durchgeführt.
- Die Auswahl des Client- oder Coordinatortyps wird nun unmittelbar beim Erstellen des Netzwerkknotens durchgeführt. Nach dem Erstellen des Knotens kann sein Typ nicht mehr geändert werden.

Abbildung 6. Erstellen des neuen Netzwerkknotens

- Die Konfiguration der IP-Adressen und DNS-Namen der Clients sowie die Konfiguration der externen IP-Adressen der Client-Firewalls ist nicht mehr erforderlich.
- Als IP-Adressenserver für die Clients werden standardmäßig ihre Coordinatoren verwendet. Es ist nicht mehr nötig, den IP-Adressenserver in der Registerkarte **IP-Adressen** anzugeben.
- Die Konfiguration der Speicherung des Passworts auf den Knoten wurde vereinfacht und wird nun auf der Registerkarte **Schlüssel** durchgeführt.

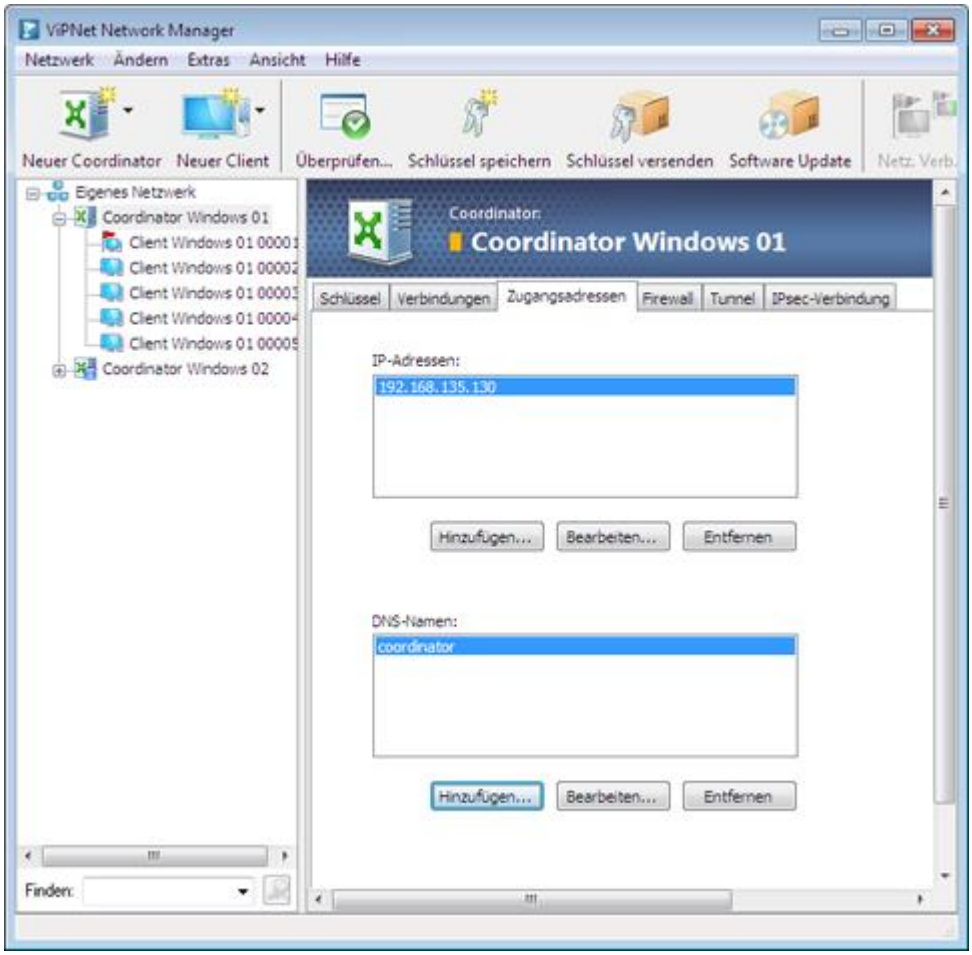

Abbildung 7. Zugangsadressen des Coordinators

Keine Funktion zur Verwaltung der Berechtigungen

Früher wurden im Programm ViPNet Network Manager die Berechtigungen der ViPNet Netzwerkbenutzer konfiguriert. Nun wird diese Funktionalität nicht mehr verwendet. Standardmäßig wird den Coordinatoren des Netzwerks die Berechtigungsstufe „Standardmodus“, den Clients die Berechtigungsstufe „Eingeschränkter Modus“ zugewiesen. Auf den Coordinatoren kann die Berechtigungsstufe vom Netzwerkknotenadministrator geändert werden. Beim Update von ViPNet VPN auf die Version 4.2 wird allen Clients die Berechtigungsstufe „Eingeschränkter Modus“ zugewiesen. Auf den Coordinatoren wird die zuvor eingestellte Berechtigungsstufe beibehalten.

Definition der DNS-Serverliste

Es kann nun eine Liste von DNS-Servern festgelegt werden, die auf den Knoten des lokalen ViPNet Netzwerks installiert sind. Als DNS-Server können folgende Knotentypen auftreten:

- ViPNet Coordinator (Windows).
- ViPNet Coordinator HW/VA.

- ViPNet Client (Windows) einschließlich des Knotens, auf dem der Manager-Arbeitsplatz eingerichtet ist.

Knoten, die von Coordinatoren getunnelt werden, können ebenfalls als DNS-Server auftreten.

Definition der Netzwerkeinstellungen von ViPNet Coordinator HW/VA

Es besteht nun die Möglichkeit, die Netzwerkeinstellungen für den Coordinator ViPNet Coordinator HW/VA im Programm ViPNet Network Manager zu konfigurieren. Sie können dort die Parameter der Netzwerkadapter von ViPNet Coordinator HW/VA angeben und die Routen für die Weiterleitung des Traffics über diesen Coordinator definieren. Die aktualisierten Einstellungsdaten von ViPNet Coordinator HW/VA werden als Bestandteil von Adresslisten weitergeleitet.

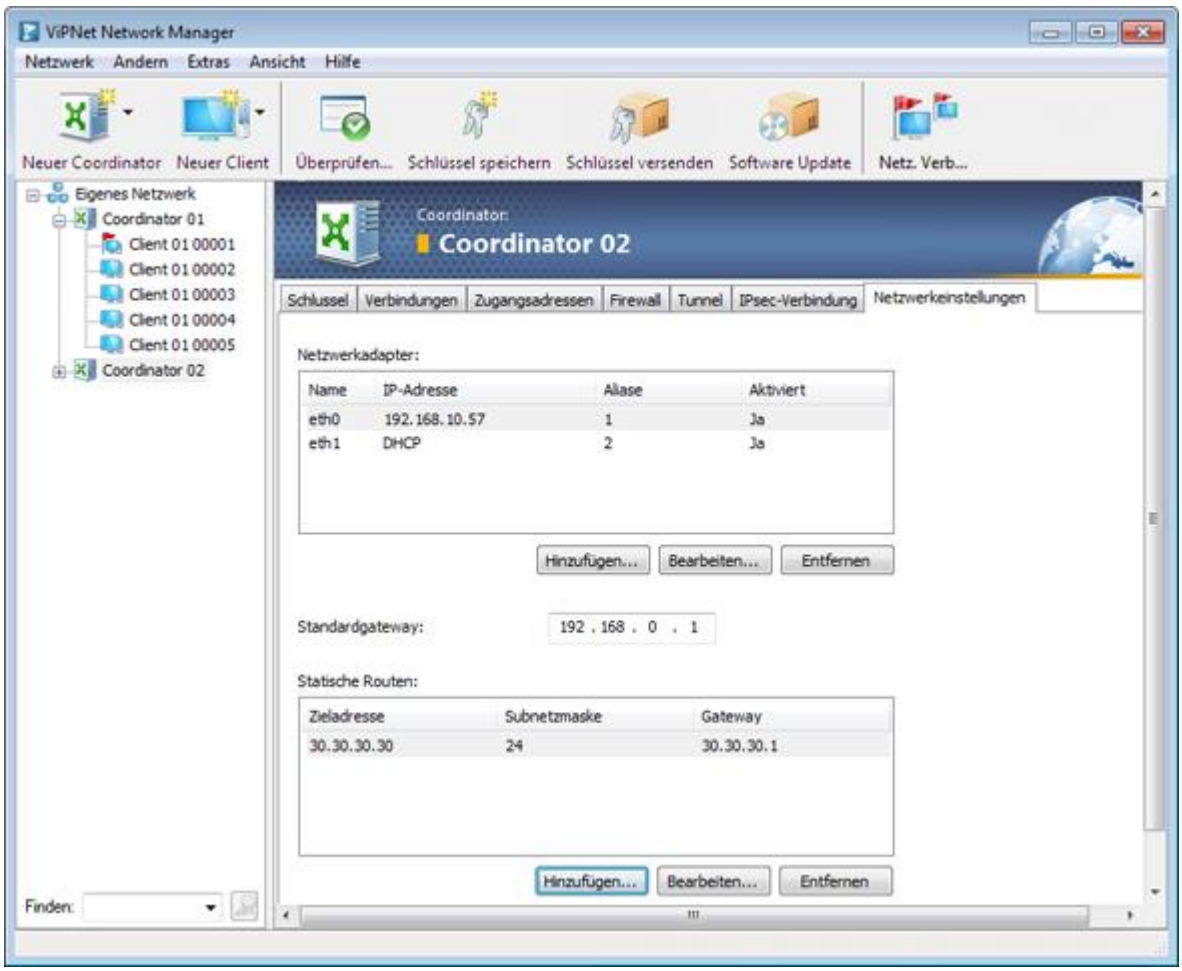

Abbildung 8. Konfiguration von ViPNet Coordinator HW/VA

Vereinfachte Konfiguration der Firewall für Clients

Die Verbindung der Clients über eine Firewall zu einem externen Netzwerk wird jetzt automatisch durch das Programm ViPNet Network Manager konfiguriert. Die Einstellungen hängen dabei vom Client-Typen ab:

- Für alle Clients wird die Verbindung über eine Firewall mit dynamischem NAT konfiguriert.
- Für Clients ViPNet Client for Android und ViPNet Client für Mac OS X wird zusätzlich die Weiterleitung des Datenverkehrs über ihren Coordinator konfiguriert.

Diese Änderungen hängen damit zusammen, dass im ViPNet Netzwerk neue Technologien für Verbindungen zwischen den Knoten verwendet werden. Jetzt wird nicht unterstützt, dass sich Clients in anderen Modi über eine Firewall zu einem externen Netzwerk verbinden.

Wird das Programm ViPNet Network Manager auf die Version 4.4 aktualisiert, werden abweichende Verbindungseinstellungen über eine Firewall für alle Clients gemäß den neuen Anforderungen angepasst.

Entsprechende Änderungen sind bereits in der Oberfläche des ViPNet Network Manager vorgenommen, d.h. die Registerkarte **Firewall** für Clients wurde gelöscht.

Änderungen in der IPsec-Konfiguration für Netzwerkknoten ViPNet Coordinator HW/VA

In früheren Versionen konnte die IP-Adresse bzw. der DNS-Name für Netzwerkknoten ViPNet Coordinator HW/VA, die als IPsec-Gateways im Einsatz sind, nur für Verbindungen mit Smartphone-Clients festgelegt werden. Nun kann die Adresse auch bei einer IPsec-Verbindung mit dem betroffenen Netzwerk definiert werden. Dadurch können Netzwerkknoten ViPNet Coordinator HW/VA, die sich hinter einer Firewall mit NAT befinden, als IPsec-Gateways für Verbindungen zu anderen Netzwerken eingesetzt werden.

Konfiguration der Liste der verwalteten Knoten für das ViPNet Policy Manager

Erlauben Sie die Nutzung der Software ViPNet Policy Manager auf dem Client, ist es erforderlich, die Liste der Netzwerkknoten anzugeben, deren Sicherheitslinien Sie mit Hilfe des ViPNet Policy Managers verwalten können. Diese Einstellung ist in der Registerkarte **Verwaltete Netzwerkknoten** erforderlich.

Erstmaliger Start des Programms ViPNet Network Manager ohne Netzwerk-Erstellung

Beim erstmaligen Starten des Programms ViPNet Network Manager musste zuvor sofort die Netzwerkstruktur mit Hilfe des ViPNet Netzwerkaufbauassistenten erstellt werden. Nun können Sie diesen Schritt überspringen und sofort zum Hauptfenster des Programms wechseln. Klicken Sie dazu im Assistentenfenster auf die Schaltfläche **Schließen**. Dabei wird eine Mindeststruktur des Netzwerks angelegt (ein Coordinator und ein Client, der als Manager-Arbeitsplatz festgelegt wird) und das Hauptfenster von ViPNet Network Manager geöffnet.

Keine Funktion zum Erstellen des Stammzertifikats

Da die Public-Key-Infrastruktur (PKI) nicht in ViPNet VPN-Netzwerken verwendet wird, besteht auch keine Notwendigkeit, Stammzertifikate für den Administrator des Netzwerks zu erstellen. Beim Aufbau des Netzwerks und der Knotenschlüssel im Programm ViPNet Network Manager wird nun kein Stammzertifikat mehr angelegt.

Möglichkeit zur Änderung des Benutzerpassworts während beliebiger Sitzung im Programm ViPNet Network Manager

Im Programm ViPNet Network Manager konnten die Benutzerpasswörter zuvor ausschließlich in der Programmsitzung geändert werden, in welcher die Netzwerkknoten erstellt wurden. Nun wurde diese Einschränkung aufgehoben. Wenn eine Schlüsseldistribution auf dem Knoten bereits installiert ist, dann wird nach dem Passwortwechsel zusammen mit dem Schlüsselupdate eine Benachrichtigung an den Client gesendet, dass der Benutzer sein Passwort selbständig ändern sollte. Das Passwort, das vom Administrator im Programm ViPNet Network Manager definiert wurde, wird nicht an den Knoten weitergeleitet.

Anzeige und Wechsel des Netzwerkknotenadministrator-Passworts

In den vorhergehenden Versionen des Programms ViPNet Network Manager wurde das Passwort des Netzwerkknotenadministrators ausschließlich in der Datei `ViPNet_a.txt` gespeichert, die gleichzeitig mit den Netzwerkknotenschlüsseln automatisch erstellt wurde und nicht geändert werden konnte. In Version 4.2.2 besteht die Möglichkeit, das Passwort im Programm ViPNet Network Manager anzuzeigen und zu ändern. Die Datei `ViPNet_a.txt` wird nicht mehr angelegt.

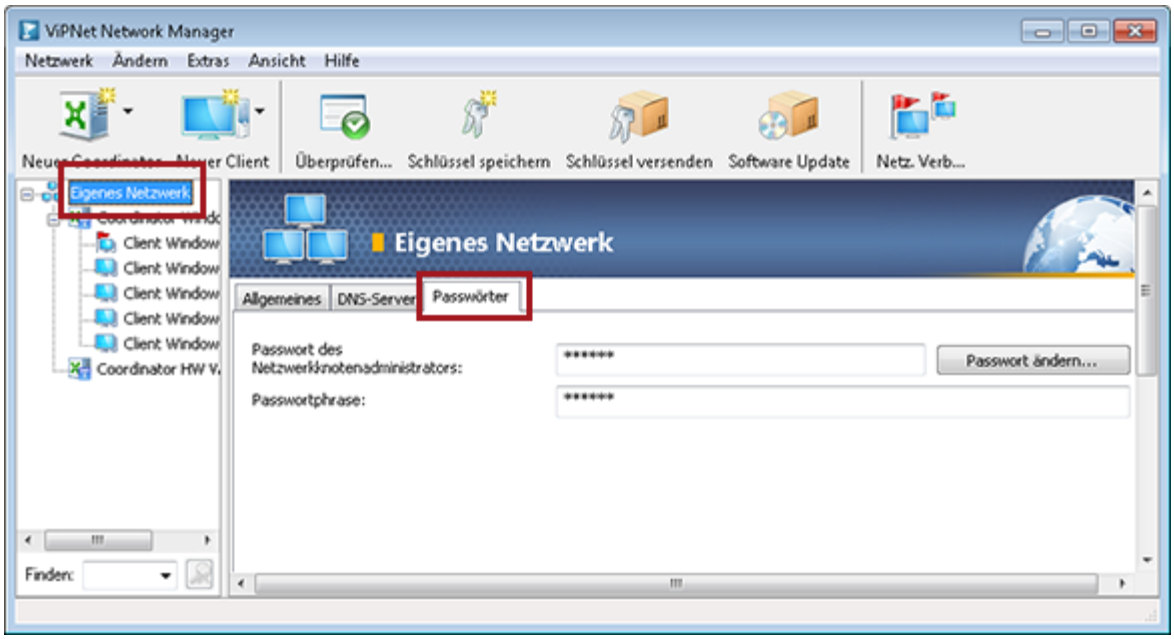

Abbildung 9. Wechsel des Netzwerkknotenadministrator-Passworts

Wechsel des Internetzwerk-Masterschlüssels

Damit die Sicherheit der Partnernetzwerk-Kommunikation erhöht wird, gibt es nun die Möglichkeit der Änderung des Internetzwerk-Masterschlüssels, der für abgesicherte Partnernetzwerk-Verbindungen verwendet wird.

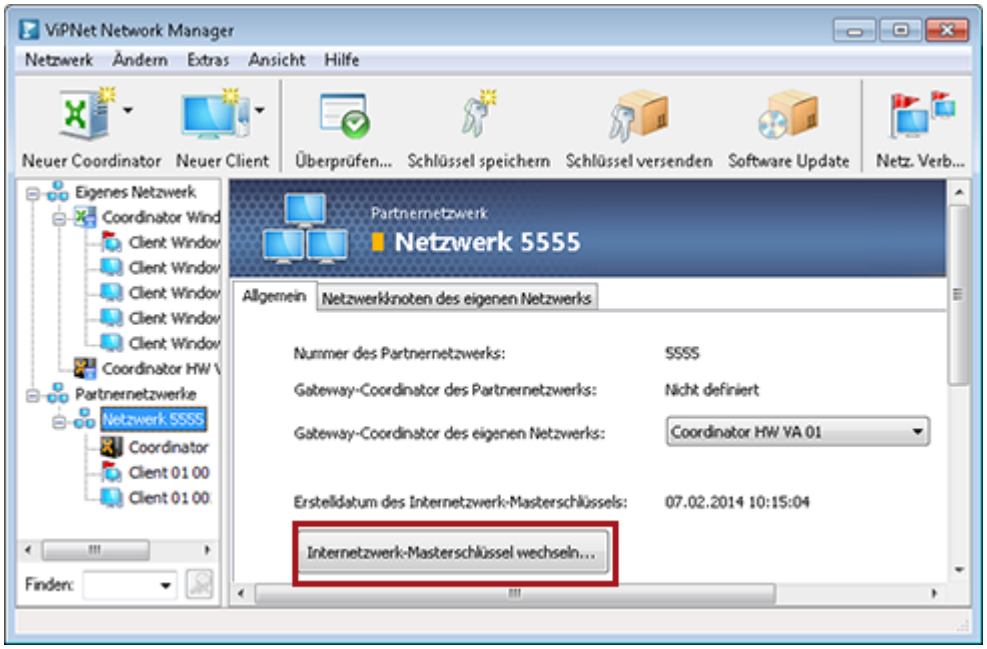

Abbildung 10. Wechsel des Internetzwerk-Masterschlüssels

Möglichkeit zum Deaktivieren der Überprüfung der Datenvollständigkeit

Während der Konfiguration und Bearbeitung der Netzwerkstruktur deckt das Programm ViPNet Network Manager mögliche Konflikte auf und weist auf fehlende Daten hin. Nun besteht die Möglichkeit, diese Prüfung auf unvollständige Daten zu deaktivieren, damit erfahrene ViPNet Netzwerkadministratoren von den eingeblendeten Hinweisen nicht abgelenkt werden. Die Prüfung der Datenvollständigkeit kann im Fenster **Einstellungen** oder im Fenster **Überprüfung der ViPNet Netzwerkkonfiguration** deaktiviert werden.

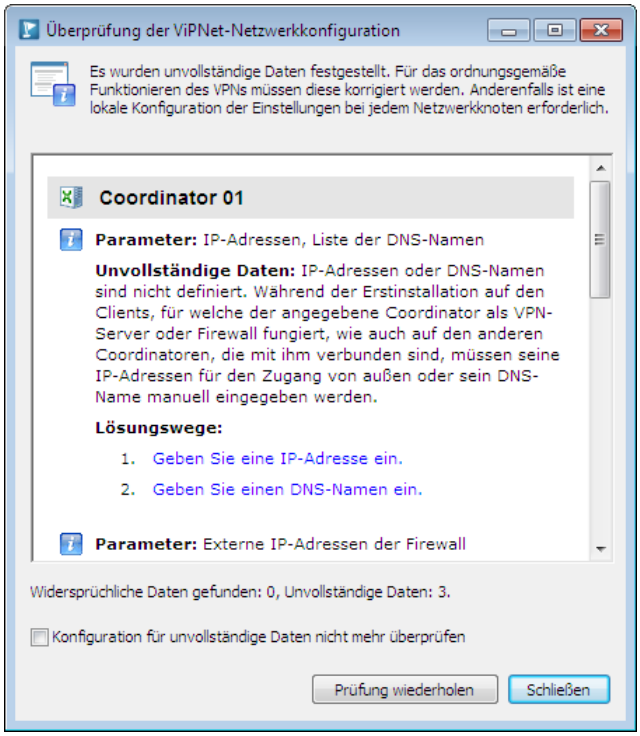
Überprüfung der ViPNet-Netzwerkkonfiguration
Es wurden unvollständige Daten festgestellt. Für das ordnungsgemäße Funktionieren des VPNs müssen diese korrigiert werden. Anderenfalls ist eine lokale Konfiguration der Einstellungen bei jedem Netzwerkknoten erforderlich.
Coordinator 01
Parameter: IP-Adressen, Liste der DNS-Namen
Unvollständige Daten: IP-Adressen oder DNS-Namen sind nicht definiert. Während der Erstinstallation auf den Clients, für welche der angegebene Coordinator als VPN-Server oder Firewall fungiert, wie auch auf den anderen Coordinatoren, die mit ihm verbunden sind, müssen seine IP-Adressen für den Zugang von außen oder sein DNS-Name manuell eingegeben werden.
Lösungswege:
1. Geben Sie eine IP-Adresse ein.
2. Geben Sie einen DNS-Namen ein.
Parameter: Externe IP-Adressen der Firewall
Widersprüchliche Daten gefunden: 0, Unvollständige Daten: 3.
Konfiguration für unvollständige Daten nicht mehr überprüfen
Prüfung wiederholen
Schließen

Abbildung 11. Deaktivieren der Überprüfung der Datenvollständigkeit

Neue Möglichkeiten von ViPNet Client und ViPNet Coordinator

Installation und Upgrade

Installation der ViPNet Software

Für die Programme ViPNet Client und ViPNet Coordinator Version 4.x wurde das Installationsprogramm überarbeitet, nämlich:

- es wurde ein MSI-Installationspaket zusammengestellt, das die Installation des Programms mit Hilfe des Microsoft System Center (s. Installation der Software unter Verwendung von Microsoft System Center auf S. 24) oder eines Anmeldeskripts logon script ermöglicht (s. Installation der Software unter Verwendung eines Anmeldeskripts auf S. 24);

- es wurden Änderungen an der Vorgehensweise bei der Installation des Programms mittels Befehlszeile vorgenommen (s. Nicht interaktiver Installationsmodus auf S. 24).

Installation der Software unter Verwendung von Microsoft System Center

Für die Programme ViPNet Client und ViPNet Coordinator Version 4.x wurden MSI-Installationspakete erarbeitet. Die Anwendung der Technologie von Windows Installer ermöglicht Gruppeninstallationen von ViPNet Software auf Computer der Windows-Domäne. Der Administrator des ViPNet Netzwerks kann mit Hilfe der Windows-Werkzeuge einzelne Pakete aus MSI-Installationsdateien erstellen und auf dem Update-Server für den weiteren Versand auf die Computer der Domäne veröffentlichen. Die Benutzer erhalten Benachrichtigungen des Software-Aktualisierungsdienstes Windows Update und können die Installation der Software selbständig einleiten.

Installation der Software unter Verwendung eines Anmeldeskripts

Dank des MSI-Installationspakets können Sie eine Gruppeninstallation der ViPNet Software mit Hilfe eines Anmeldeskripts (logon script) durchführen. Auf diese Weise kann die Software auf eine beliebige Anzahl der Computer in der Windows-Domäne gleichzeitig installiert werden. Zum Durchführen einer solchen Installation:

1. Kopieren Sie die MSI-Installationsdatei in einen Ordner, der für alle Benutzer zugänglich ist, auf deren Computer die Software installiert werden soll.
2. Konfigurieren Sie die Gruppenrichtlinie, indem Sie ein Installationspaket und ein Anmeldeskript erstellen, mit dessen Hilfe die Software auf die Benutzercomputer installiert wird.

Nicht interaktiver Installationsmodus

In Version 4.x wurde das Installationsprinzip des Programms ViPNet Monitor im nicht interaktiven Modus geändert. In Version 3.2.x wurde die Installationsdatei aus der Befehlszeile gestartet, die Installationsparameter wurden aus der Datei `silent.ini` ausgelesen. In Version 4.x erfolgen der Start der Installationsdatei und die Konfiguration der Installationsparameter direkt in der Befehlszeile. Es kann zum Beispiel angegeben werden, welche Komponenten installiert werden sollen, und ob der Computer nach der Installation des Programms zwangsweise neu gestartet werden soll.

Die Verwendung des nicht interaktiven Modus ermöglicht es Ihnen:

- eine Remote-Installation durchzuführen;
- Programme zu erstellen, die unter Verwendung der Windows-Befehlszeile eine automatische Installation der Software mit vorgegebenen Parametern starten.

Kompatibilität mit Windows

Die Programme ViPNet Client und ViPNet Coordinator Version 4.x können unter dem Betriebssystem Windows 8 (32/64-Bit) und Windows Server 2012 (64-Bit) installiert werden.

Das Programm ViPNet Policy Manager ist mit dem Betriebssystem Windows 7 oder höher kompatibel.

Deaktivierungslogik der Windows Firewall

Bei der Installation und der anschließenden Verwendung der Programme ViPNet Client und ViPNet Coordinator 4.x bleibt die Standardfirewall von Windows aktiviert. Dadurch kann der Schutz Ihres Computers bei der Installation des Netzwerks ununterbrochen gewährleistet werden. In Version 3.2.x wurde die Firewall im Zuge der Installation der Software deaktiviert.

Installation der ViPNet Schlüssel

In ViPNet Monitor Version 4.x wird der Assistent der primären Initialisierung nicht mehr verwendet. Der Assistent für die Schlüsselinstallation ermöglicht die Durchführung aller Szenarien, die mit der Installation oder dem Wechsel der Schlüssel auf einem ViPNet Netzwerkknoten in Zusammenhang stehen, und zwar:

- Installation der ViPNet Adresslisten und -Schlüssel auf dem Netzwerkknoten;
- Hinzufügen eines neuen Benutzers auf dem Netzwerkknoten;
- Austausch des auf dem Computer installierten Netzwerkknotens;
- Wiederholte Installation der Schlüssel;
- Löschen der Adresslisten und Schlüssel aus dem Schlüsselordner des Netzwerkknotens.

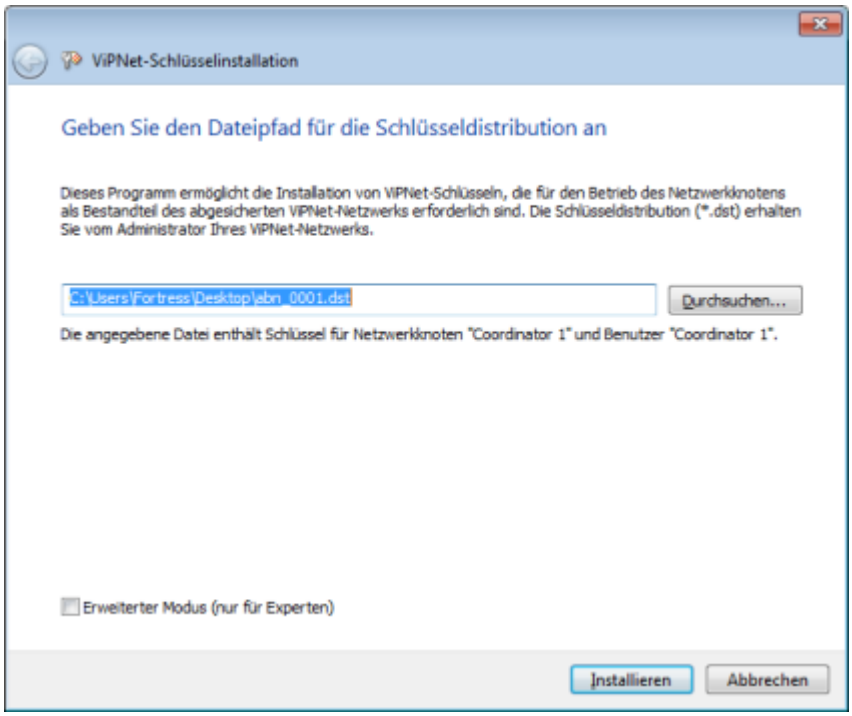
ViPNet-Schlüsselinstallation
Geben Sie den Dateipfad für die Schlüsseldistribution an
Dieses Programm ermöglicht die Installation von ViPNet-Schlüsseln, die für den Betrieb des Netzwerkknotens als Bestandteil des abgesicherten ViPNet-Netzwerks erforderlich sind. Die Schlüsseldistribution (*.dst) erhalten Sie vom Administrator Ihres ViPNet-Netzwerks.
C:\Users\Fortress\Desktop\abn_0001.dst
Durchsuchen...
Die angegebene Datei enthält Schlüssel für Netzwerkknoten "Coordinator 1" und Benutzer "Coordinator 1".
Erweiterter Modus (nur für Experten)
Installieren
Abbrechen

Abbildung 12. Assistent zur Installation der Schlüssel in Version 4.0

In ViPNet Client und ViPNet Coordinator Version 4.x führt der Assistent der ViPNet Schlüsselinstallation eine ausführlichere Analyse der Daten, die in der Schlüsseldistribution enthalten sind, und der Dateien im Schlüsselordner des Netzwerkknotens durch.

ViPNet Updatesystem

In ViPNet Monitor 3.2.x werden Informationen über eingetroffene Updates der Software oder der Adresslisten und Schlüssel in Form von Meldungen angezeigt. Im Fenster der Meldung kann das empfangene Update angenommen oder abgelehnt werden.

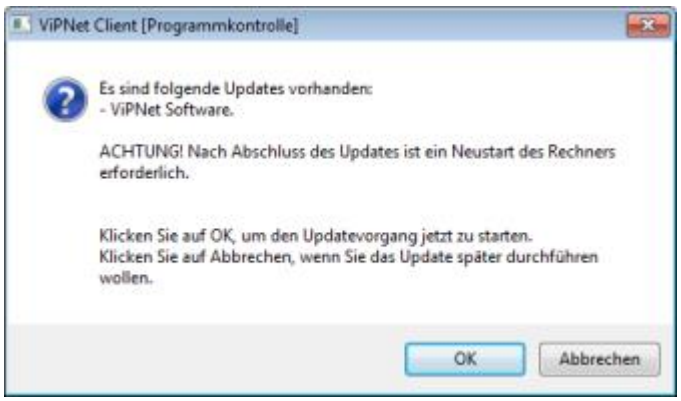
ViPNet Client [Programmkontrolle]
Es sind folgende Updates vorhanden:
- ViPNet Software.
ACHTUNG! Nach Abschluss des Updates ist ein Neustart des Rechners erforderlich.
Klicken Sie auf OK, um den Updatevorgang jetzt zu starten.
Klicken Sie auf Abbrechen, wenn Sie das Update später durchführen wollen.
OK
Abbrechen

Abbildung 13. Meldung über die vorhandene Software-Update-Dateien

In ViPNet Monitor der Version 4.x wird der Empfang und die Installation der Updates mit Hilfe des ViPNet Update Systems durchgeführt. Beim gemeinsamen Einsatz mit ViPNet Policy Manager werden auch die Updates der Sicherheitsrichtlinien in das Updatesystem weitergeleitet.

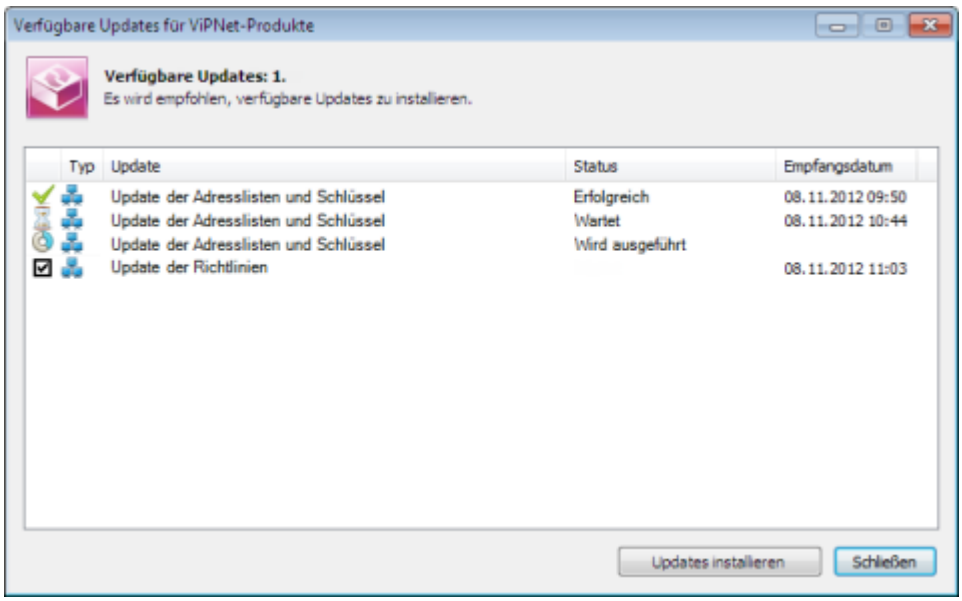

Abbildung 14. ViPNet-Updatesystem

Die Installation der Updates kann sowohl automatisch als auch manuell durchgeführt werden.

Wenn auf dem Knoten die automatische Installation von Updates eingestellt ist, dann werden alle Aktionen vom ViPNet Updatesystem im „leisen“ Modus ohne Ausgabe irgendwelcher Meldungen auf dem Bildschirm durchgeführt. Wenn die manuelle Installation von Updates eingestellt ist, dann wird beim Empfang von Updatedateien im Infobereich der Taskleiste eine entsprechende Meldung angezeigt.

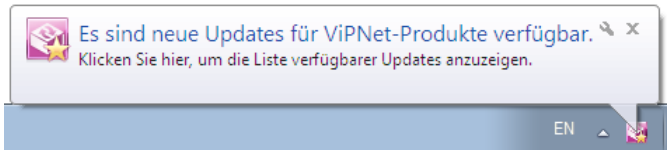

Abbildung 15. Im Infobereich eingeblendete Benachrichtigung über vorhandene Updates

Traffic-Schutz

Filterung des Traffics

In diesem Abschnitt werden die Verbesserungen und Weiterentwicklungen des Programms ViPNet Client und ViPNet Coordinator beschrieben, welche die Filterung des Traffics, die Übersetzung von IP-Adressen und die Kompatibilität mit dem Programm ViPNet Policy Manager zwecks einer zentralisierten Verwaltung von Sicherheitsrichtlinien betreffen.

Empfang von Sicherheitsrichtlinien aus ViPNet Policy Manager

In ViPNet Monitor können Netzwerkfilter und Regeln der Netzwerkadressenübersetzung (NAT) angewendet werden, die im Programm ViPNet Policy Manager erstellt wurden. Das Programm ViPNet Policy Manager ist dafür bestimmt, die Sicherheitsrichtlinien der Knoten im geschützten ViPNet Netzwerk zentralisiert zu verwalten. ViPNet Policy Manager ermöglicht es, unterschiedliche Sicherheitsrichtlinien sowohl für einzelne Netzwerkknoten als auch für Knotengruppen zu definieren und zentralisiert zu versenden.

Abbildung 16. Versand von Sicherheitsrichtlinien

Sobald auf einem Netzwerkknoten Sicherheitsrichtlinien von ViPNet Policy Manager eintreffen, erhält der Benutzer eine Benachrichtigung des ViPNet Update Systems.

Wenn der Benutzer das Update der Sicherheitsrichtlinie auf seinem Netzwerkknoten bestätigt, dann wird das Programm ViPNet Monitor neu gestartet. Anschließend wird die neue Sicherheitsrichtlinie auf den Netzwerkknoten angewendet. Die als Inhalt der Richtlinie erhaltenen Regeln und Filter können nicht geändert werden.

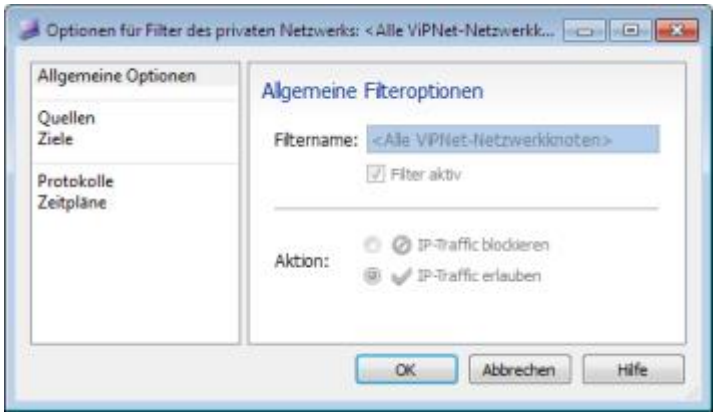

Abbildung 17. Optionen eines Netzwerkfilters, der in ViPNet Policy Manager erstellt wurde

Wenn Sie nicht möchten, dass auf den Knoten Sicherheitsrichtlinien angewendet werden, die aus dem Programm ViPNet Policy Manager gesendet wurden, dann beim Arbeit im Administratormodus deaktivieren Sie in Gruppe **Sicherheitsrichtlinien** das Kontrollkästchen **Sicherheitsrichtlinien übernehmen**.

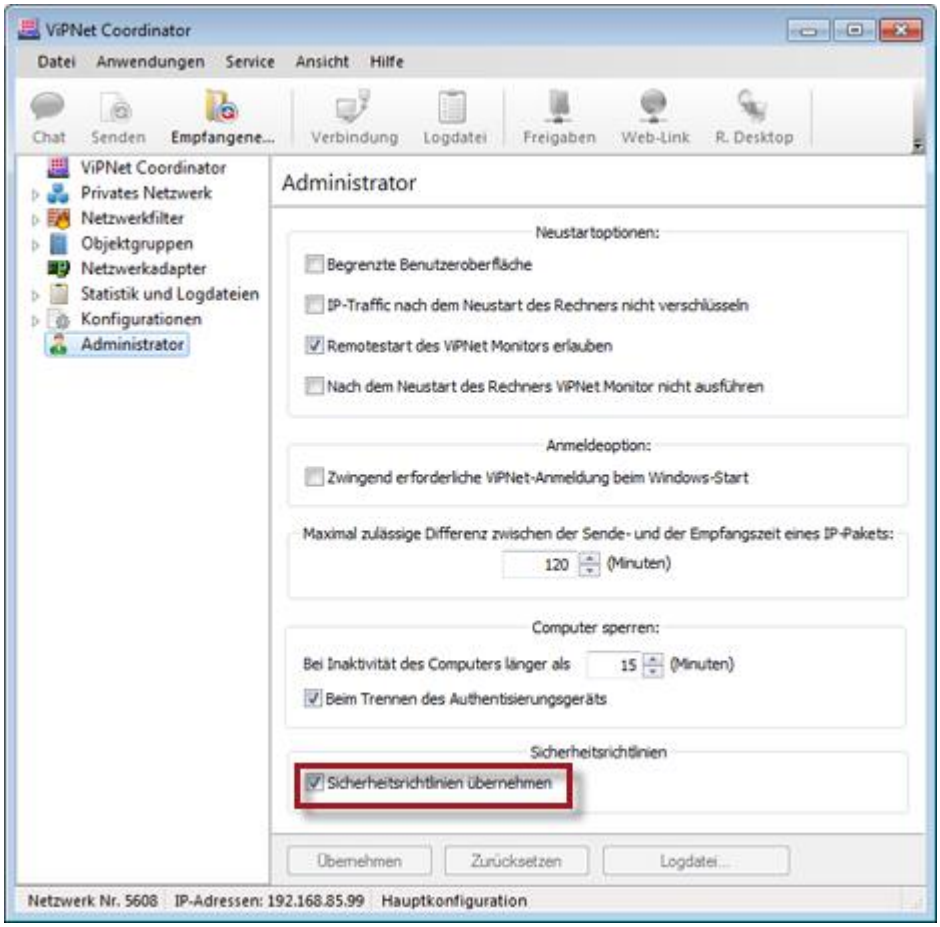

Abbildung 18. Einstellung von Sicherheitsrichtlinienanwendung

Bereits angenommene Sicherheitsrichtlinien werden in diesem Fall wieder außer Kraft gesetzt (Netzwerkfilter, die als Bestandteil von Richtlinien übernommen wurden, werden ausgeblendet und deaktiviert). Zusätzlich wird der ViPNet Policy Manager-Knoten darüber informiert, dass neue Sicherheitsrichtlinien vom gegebenen Netzwerkknoten nicht mehr angenommen werden.

Wenn das Kontrollkästchen **Sicherheitsrichtlinien übernehmen** im Nachhinein wieder aktiviert wird, dann werden bereits angenommene Richtlinien wieder aktiviert, der Empfang neuer Richtlinien aus dem Programm ViPNet Policy Manager wird wieder aufgenommen.

Neues, mit ViPNet Policy Manager kompatibles Filterformat

In diesem Abschnitt werden die Verbesserungen und Weiterentwicklungen des Programms ViPNet Client und ViPNet Coordinator beschrieben, welche die Filterung des Traffics, die Übersetzung von IP-Adressen und die Kompatibilität mit dem Programm ViPNet Policy Manager zwecks einer zentralisierten Verwaltung von Sicherheitsrichtlinien betreffen. Ausführliche Informationen zu den Besonderheiten der Netzwerkfilter und NAT-Regeln in Version 4.x s. Abschnitt Besonderheiten des Filterformats der Version 4.x im Vergleich zu Version 3.2.x (auf S. 31). Aus Gründen der Übersichtlichkeit und zur Erleichterung der Arbeit mit Regeln und Filtern wurde die Anzeige der Filter in den Programmen ViPNet Monitor und ViPNet Policy Manager vereinheitlicht.

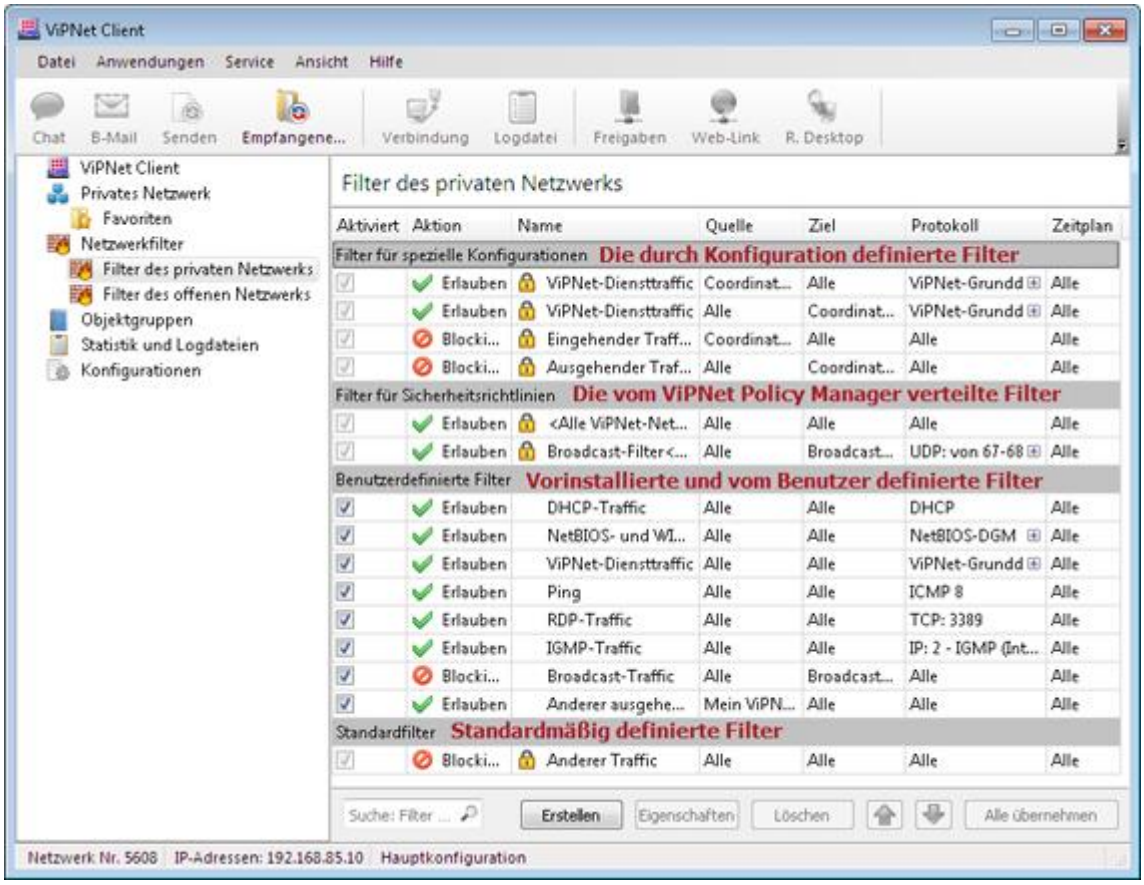
ViPNet Client
Datei Anwendungen Service Ansicht Hilfe
Chat B-Mail Senden Empfangene... Verbindung Logdatei Freigaben Web-Link R. Desktop
ViPNet Client
Privates Netzwerk
Favoriten
Netzwerkfilter
Filter des privaten Netzwerks
Filter des offenen Netzwerks
Objektgruppen
Statistik und Logdateien
Konfigurationen
Filter des privaten Netzwerks
Aktiviert Aktion Name Quelle Ziel Protokoll Zeitplan
Filter für spezielle Konfigurationen Die durch Konfiguration definierte Filter
Filter für Sicherheitsrichtlinien Die vom ViPNet Policy Manager verteilte Filter
Benutzerdefinierte Filter Vorinstallierte und vom Benutzer definierte Filter
Standardfilter Standardmäßig definierte Filter
Suche: Filter ... Erstellen Eigenschaften Löschen Alle übernehmen
Netzwerk Nr. 5608 IP-Adressen: 192.168.85.10 Hauptkonfiguration

Abbildung 19. Anzeige der Netzwerkfilter im Programm ViPNet Monitor

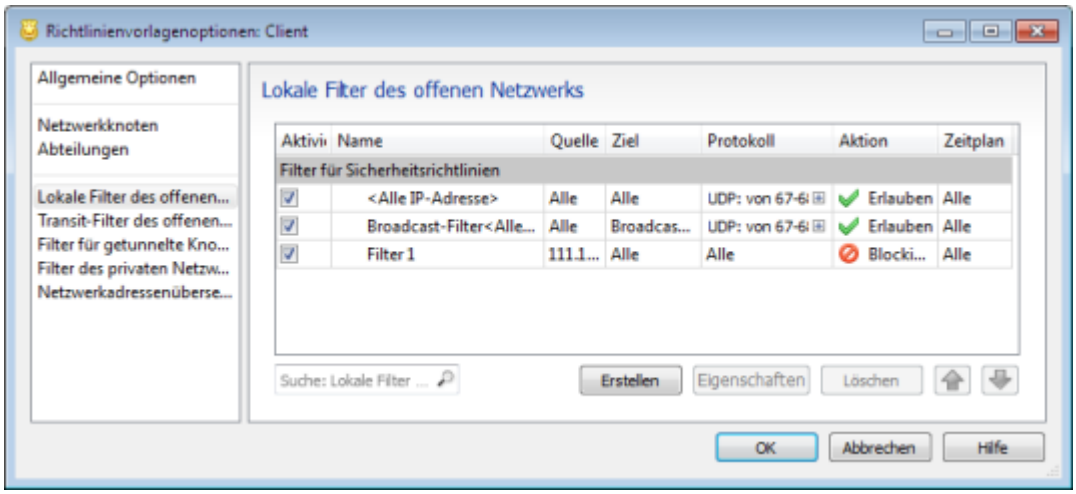
Richtlinienvorlagenoptionen: Client
Allgemeine Optionen
Netzwerkknoten
Abteilungen
Lokale Filter des offenen...
Transit-Filter des offenen...
Filter für getunnelte Kno...
Filter des privaten Netzw...
Netzwerkadressenüberse...
Lokale Filter des offenen Netzwerks
Aktivi Name Quelle Ziel Protokoll Aktion Zeitplan
Filter für Sicherheitsrichtlinien
<Alle IP-Adresse> Alle Alle UDP: von 67-6 Erlauben Alle
Broadcast-Filter<Alle... Alle Broadcas... UDP: von 67-6 Erlauben Alle
Filter 1 111.1... Alle Alle Blocki... Alle
Suche: Lokale Filter ... Erstellen Eigenschaften Löschen
OK Abbrechen Hilfe

Abbildung 20. Anzeige der Netzwerkfilter im Programm ViPNet Policy Manager

Durch den Einsatz von Sicherheitsrichtlinien, die im Programm ViPNet Policy Manager erstellt wurden, hat sich auch die Reihenfolge der Anwendung von Netzwerkfiltern und NAT-Regeln verändert. Details s. Abschnitt Priorität der Filter (s. Priorität der Netzwerkfilter auf S. 36).

Beim Erstellen der Netzwerkfilter und NAT-Regeln in den Programmen ViPNet Monitor und ViPNet Policy Manager können Objektgruppen bei der Konfiguration der einzelnen Parameter verwendet werden (s. Objektgruppen auf S. 38). Es kann zum Beispiel eine Netzwerkknoten-Gruppe oder Adress-Gruppe als Quelle oder Ziel festgelegt werden.

Besonderheiten des Filterformats der Version 4.x im Vergleich zu Version 3.2.x

Infolge der Einführung des neuen Filterformats werden die bestehenden Regeln zur Traffic-Filterung der Version 3.2.x bei einem Update der Programme ViPNet Client und ViPNet Coordinator auf die Version 4.x in Netzwerkfilter und NAT-Regeln der Version 4.x konvertiert. Im Rahmen der Konvertierung der Filterregeln wird das Format der Regeln geändert, der Inhalt bleibt jedoch erhalten. Deswegen sind nach der Umstellung auf das neue Format keine weiteren Aktionen seitens der Benutzer erforderlich.

Einige Besonderheiten des neuen Formats der Netzwerkfilter und NAT-Regeln:

- **Neuer Ansatz beim Definieren der Regeln und Filter**

  Im Programm ViPNet Monitor Version 3.2.x sollten zum Filtern des Traffic zunächst eine Traffic-Filterregel erstellt und dann im Rahmen dieser Regel die einzelnen Filter definiert werden.

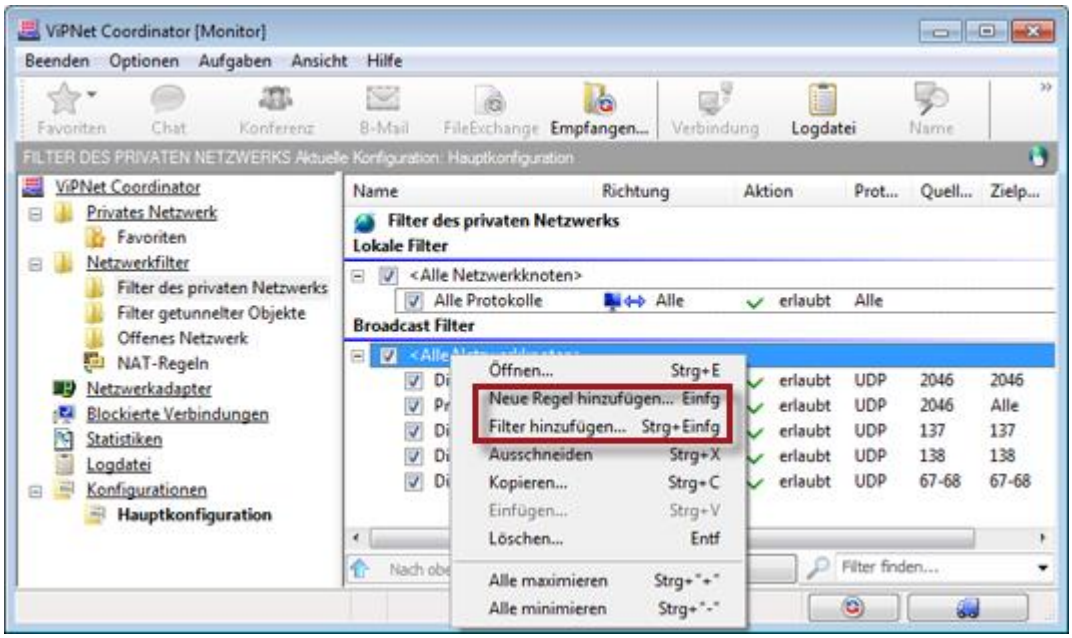

Abbildung 21. Erstellen der Regel und Filter

Für die Version 4.x wurden die Regeln und Filter zusammengeführt und werden nun als Netzwerkfilter bezeichnet. Das Konzept der Filterregel wird nicht mehr unterstützt. In beiden Versionen können NAT-Regeln für IP-Adressen definiert werden.

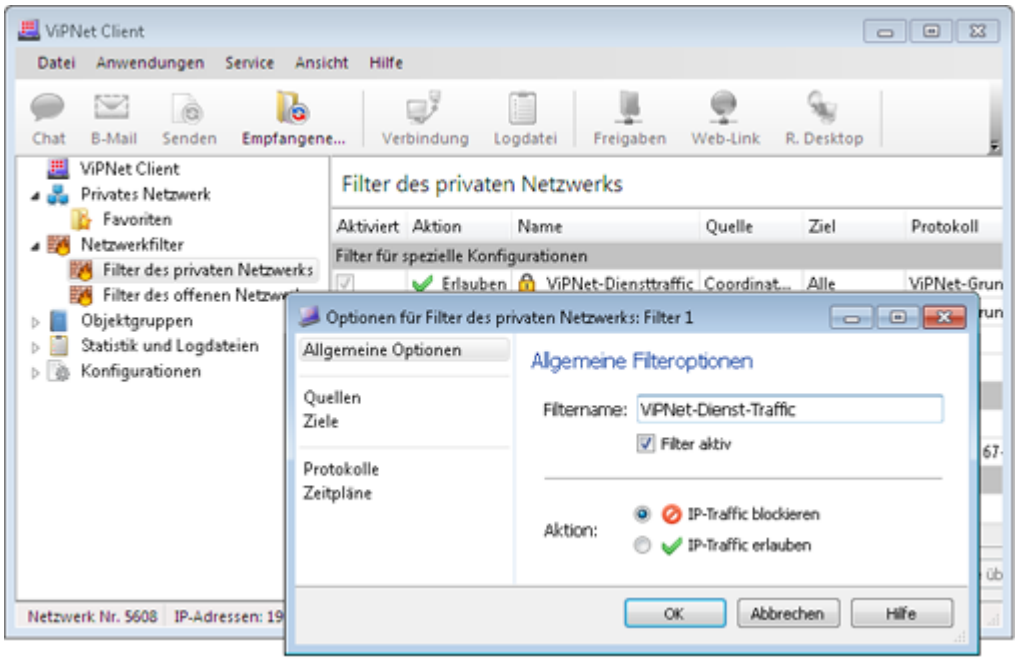

Abbildung 22. Erstellung der Filter in Version 4.x

- **Verbindungsrichtung**

  Im Programm ViPNet Monitor 3.2.x kann die Verbindungsrichtung der Filterregel als eingehend, ausgehend oder beliebig definiert werden.

  Im Programm ViPNet Monitor 4.0 können beim Erstellen der Filter die Quelle (Knoten oder Adresse des Absenders) und das Ziel (Knoten oder Adresse des Empfängers) in Form von Objektgruppen oder Systemobjekten definiert werden. Anhand dieser Angaben wird die Verbindungsrichtung bestimmt. Wenn zum Beispiel das Objekt **Mein ViPNet Knoten** als Quelle festgelegt wurde, dann werden die ausgehenden Verbindungen vom Filter erfasst. Wenn das Objekt m als Quelle ausgewählt wurde, dann werden die eingehenden Verbindungen vom Filter verarbeitet.

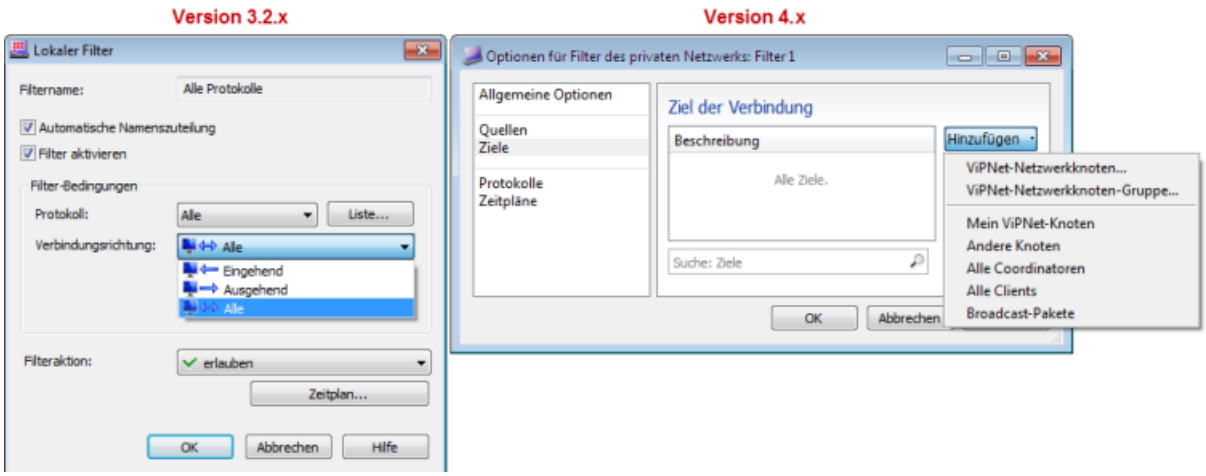

Abbildung 23. Festlegen der Richtung für die Filterung

- **NAT-Regeln**

Im Programm ViPNet Monitor 3.2.x kann beim Konfigurieren einer NAT-Regel entweder die Übersetzung der Quell-IP-Adresse (statische Regel) oder die Übersetzung der Ziel-IP-Adresse (dynamische Regel) der IP-Pakete eingestellt werden.

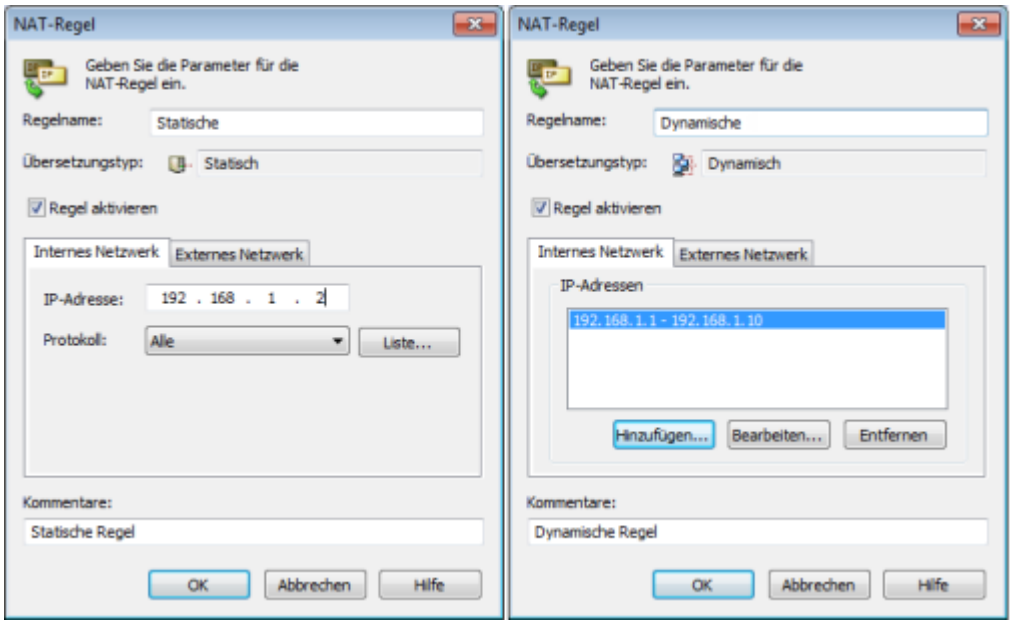

Abbildung 24. Definition von NAT-Regeln in Version 3.2.x

Im Programm ViPNet Monitor 4.x kann beim Erstellen einer NAT-Regel (s. NAT-Regeln auf S. 37) gleichzeitig die Quell- und die Zielübersetzung der IP-Pakete konfiguriert werden.

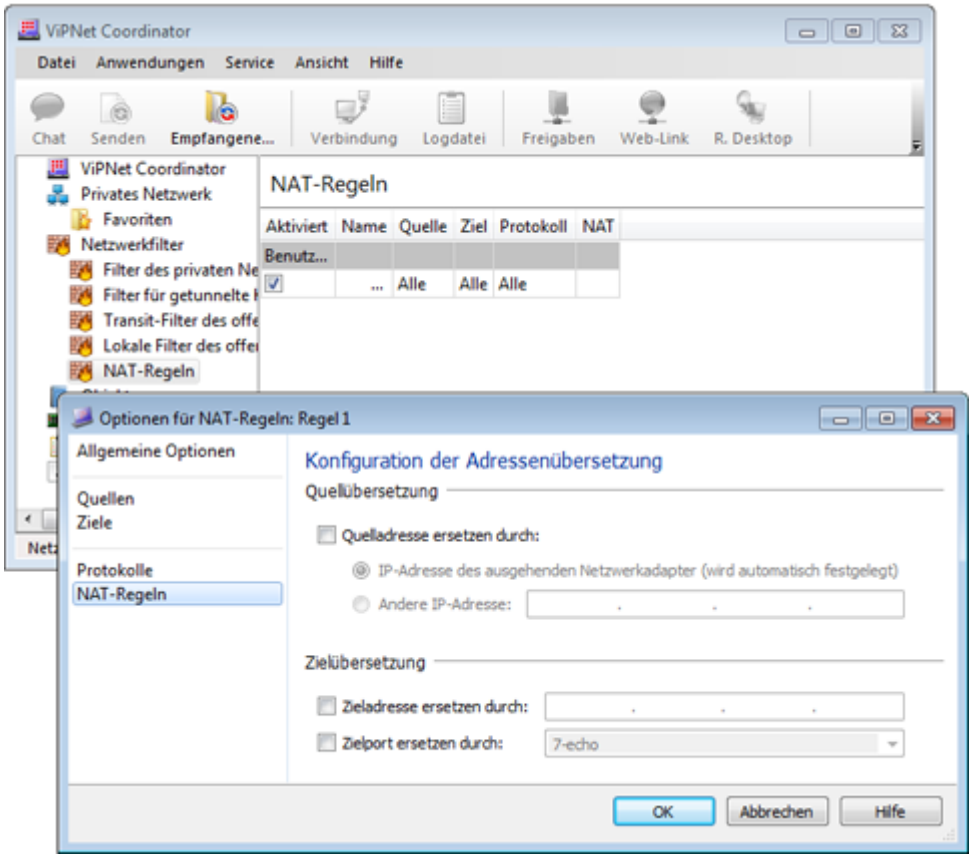

Abbildung 25. Definition von NAT-Regeln in Version 4.x

- **Zeitplan**

  Im Programm ViPNet Monitor 3.2.x kann beim Erstellen eines Zeitplans für den Filter die Zeit angegeben werden, während welcher der Filter aktiv sein soll (**Während angegebener Zeit**). Außerdem können Ausnahmen definiert werden, d. h. Zeitpläne, während welcher der Filter nicht aktiv sein wird (**Außer angegebener Zeit**).

  Im Programm ViPNet Monitor 4.x werden die Ausnahmen nicht mehr in den Netzwerkfilter-Eigenschaften, sondern in den Eigenschaften der Planungs-Gruppen definiert.

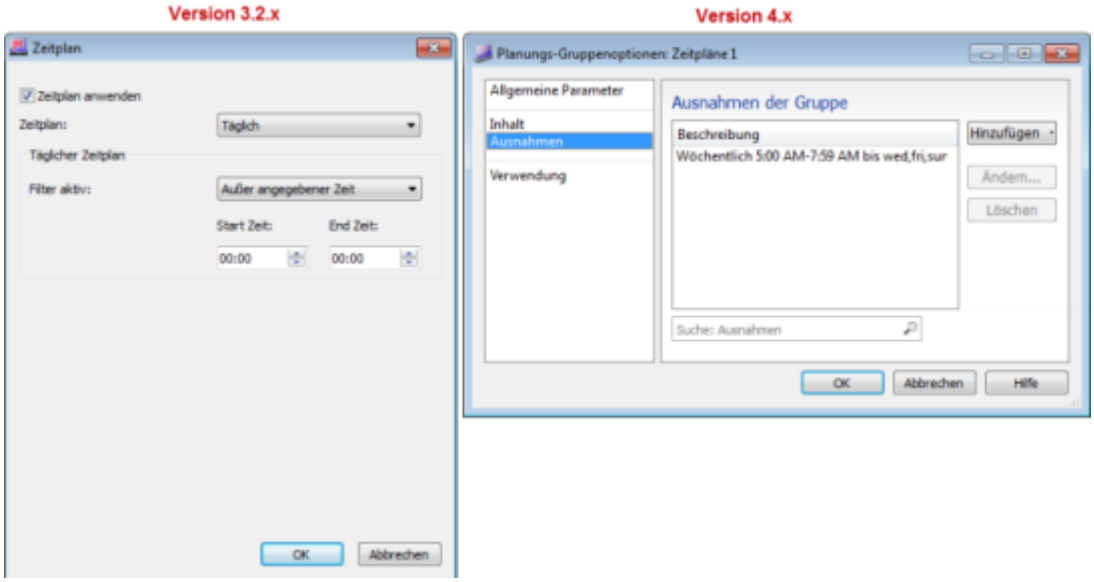

Abbildung 26. Definition einer Ausnahme im Zeitplan

- **Broadcast-Filter**

  Im Programm ViPNet Monitor 3.2.x werden die Broadcast-Filter im Bereich der Filter des privaten und des offenen Netzwerks in gesonderten Listen angezeigt.

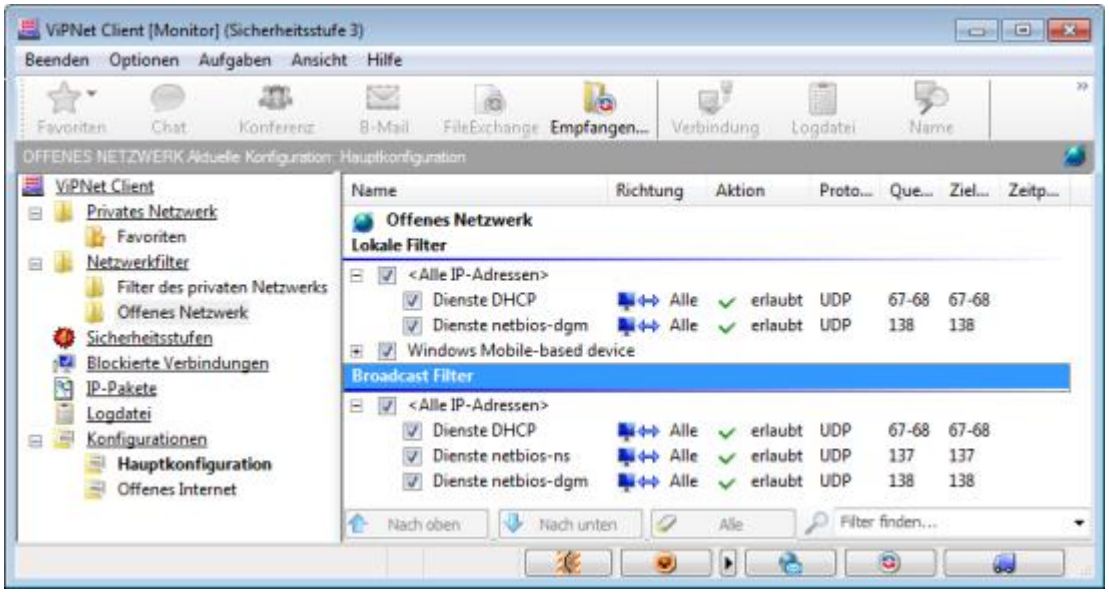

Abbildung 27. Anzeige der Broadcast-Filter in Version 3.2.x

Im Programm ViPNet Monitor 4.x werden Broadcast-Filter nicht als eine separate Gruppe geführt, sondern in der allgemeinen Filterliste des privaten oder offenen Netzwerks angezeigt. Beim Erstellen eines Broadcast-Filters sollte als Ziel der Wert **Broadcast-Adressen** ausgewählt werden.

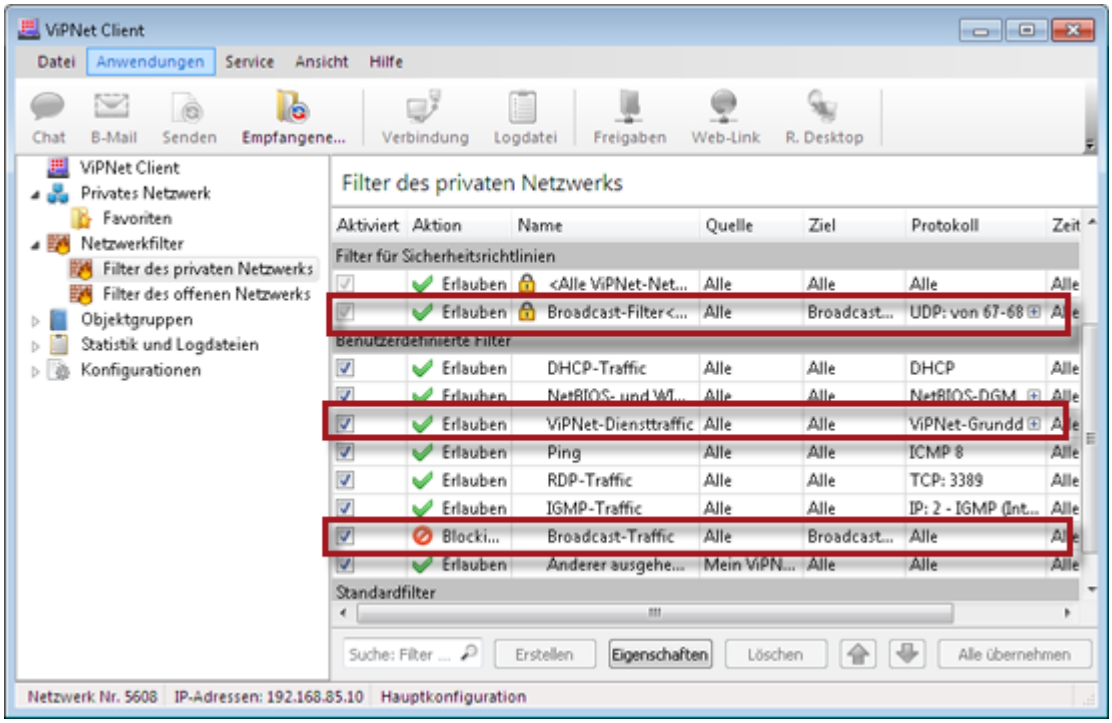

Abbildung 28. Anzeige der Broadcast-Filter in Version 4.x

Priorität der Netzwerkfilter

Im Programm ViPNet Monitor Version 4.x werden die Netzwerkfilter und NAT-Regeln absteigend (von oben nach unten) in Übereinstimmung mit den Filterlisten angewendet. Die Listen der Netzwerkfilter werden im Hauptfenster des Programms im Bereich **Netzwerkfilter** angezeigt.

Filter, die von speziellen Programmkonfigurationen abhängig sind, werden ihrer Priorität nach höher eingestuft als alle anderen Filter und deswegen vorrangig angewendet. Diese Filter können ausschließlich im Programm ViPNet Client Monitor verwendet werden. Sie können nicht geändert oder gelöscht werden. Filter, die vom Programm ViPNet Policy Manager versendet wurden, folgen ihrer Priorität nach den Filtern der Konfigurationen und können ebenfalls nicht gelöscht oder geändert werden. Es folgen Filter, die vom Benutzer im Programm ViPNet Monitor definiert wurden, sowie die vorinstallierten Filter des Programms. Bei Vorliegen bestimmter Berechtigungen können diese Filter geändert oder gelöscht werden. Am Schluss befinden sich die Standardfilter. Diese Kategorie wird durch einen Netzwerkfilter vertreten, der den gesamten IP-Traffic blockiert, der von keinem einzigen Netzwerkfilter der oberen Kategorien erfasst wurde.

Die Reihenfolge der Anwendung der Netzwerkfilter gemäß ihrer Priorität im Programm ViPNet Client Monitor ist in der Abbildung unten dargestellt.

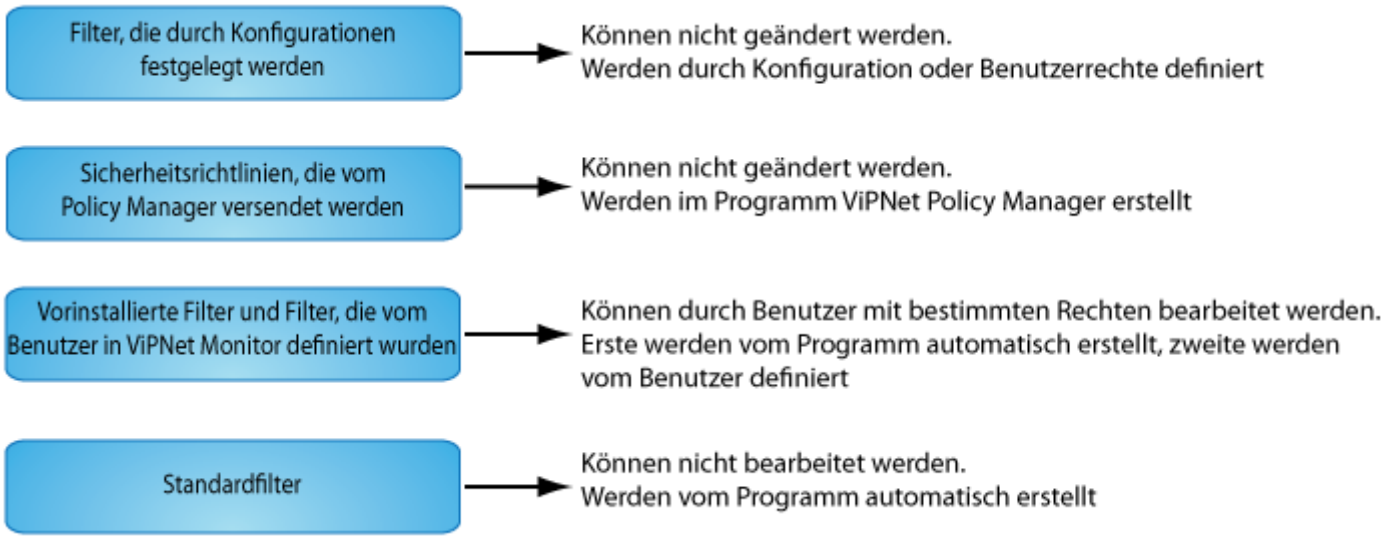
Filter, die durch Konfigurationen festgelegt werden
Können nicht geändert werden.
Werden durch Konfiguration oder Benutzerrechte definiert
Sicherheitsrichtlinien, die vom Policy Manager versendet werden
Können nicht geändert werden.
Werden im Programm ViPNet Policy Manager erstellt
Vorinstallierte Filter und Filter, die vom Benutzer in ViPNet Monitor definiert wurden
Können durch Benutzer mit bestimmten Rechten bearbeitet werden.
Erste werden vom Programm automatisch erstellt, zweite werden vom Benutzer definiert
Standardfilter
Können nicht bearbeitet werden.
Werden vom Programm automatisch erstellt

Abbildung 29. Priorität der Anwendung der Netzwerkfilter

Hinweis. Im Programm ViPNet Coordinator Monitor werden Konfigurationsfilter nicht verwendet. Die Sicherheitsrichtlinien von Policy Manager und die vom Benutzer definierten Filter werden in Übereinstimmung mit der Priorität angewendet, die in der Abbildung dargestellt ist.

NAT-Regeln

Durch Angabe der Quell- und der Zielübersetzung innerhalb einer Regel besteht nun die Möglichkeit, mehrere Netzwerksegmente über einen Coordinator kommunizieren zu lassen, der gleichzeitig die Übersetzung von IP-Adressen durchführt und die strikte Abgrenzung dieser Netzwerke voneinander gewährleistet. Somit sind Informationen über IP-Adressen, die von jedem dieser Netzwerke verwendet werden, ausschließlich auf dem Coordinator vorhanden. Diese Funktionalität kann zum Beispiel in einer DMZ-Struktur eingesetzt werden.

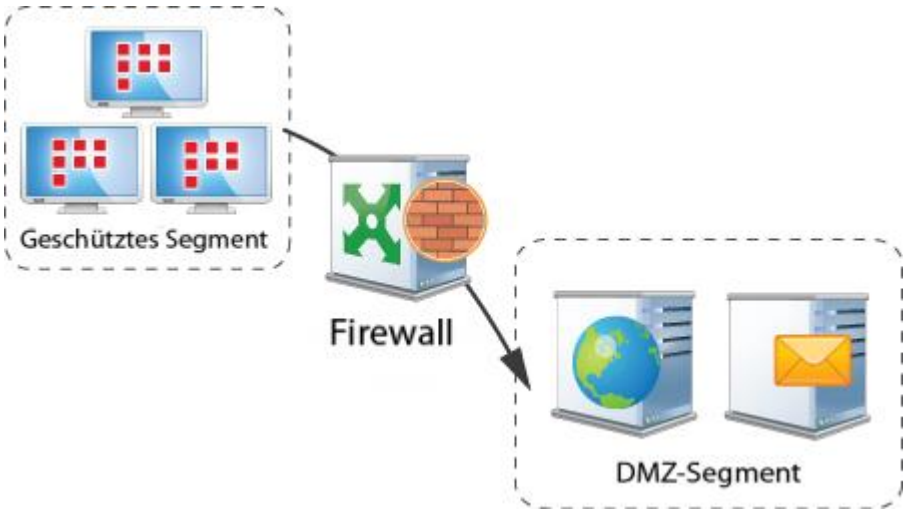

Abbildung 30. Interaktion der Netzwerksegmente in einer DMZ-Struktur

Nehmen wir an, die Netzwerkknoten des geschützten Segments bauen Verbindungen zu den Knoten des DMZ-Segments unter Verwendung der IP-Adresse des Coordinators an der Seite des geschützten Segments auf. Gemäß der NAT-Regel werden die IP-Adressen der Netzwerkknoten im geschützten Segment (Quell-IP-Adressen) in die IP-Adresse des Coordinators an der Seite des DMZ-Segments (Ziel-IP-Adresse) umgewandelt. Die IP-Adresse des Coordinators an der Seite des geschützten Segments, die als Ziel festgelegt wurde, wird in die IP-Adresse des benötigten Servers im DMZ-Segment umgewandelt.

Objektgruppen

In Version 4.x können Objektgruppen erstellt werden. Objektgruppen dienen dazu, die Definition von Netzwerkfiltern und Regeln der Adressenübersetzung im Programm ViPNet Monitor zu vereinfachen. In Objektgruppen werden mehrere Objekte eines Typs zusammengefasst, wodurch sie beim Einstellen der Filter- oder Regelparameter anstatt einzelner konkreter Objekte verwendet werden können. Objektgruppen werden beim Erstellen anderer Objektgruppen sowie beim Konfigurieren der Netzwerkfilter und NAT-Regeln im Programm ViPNet Policy Manager verwendet.

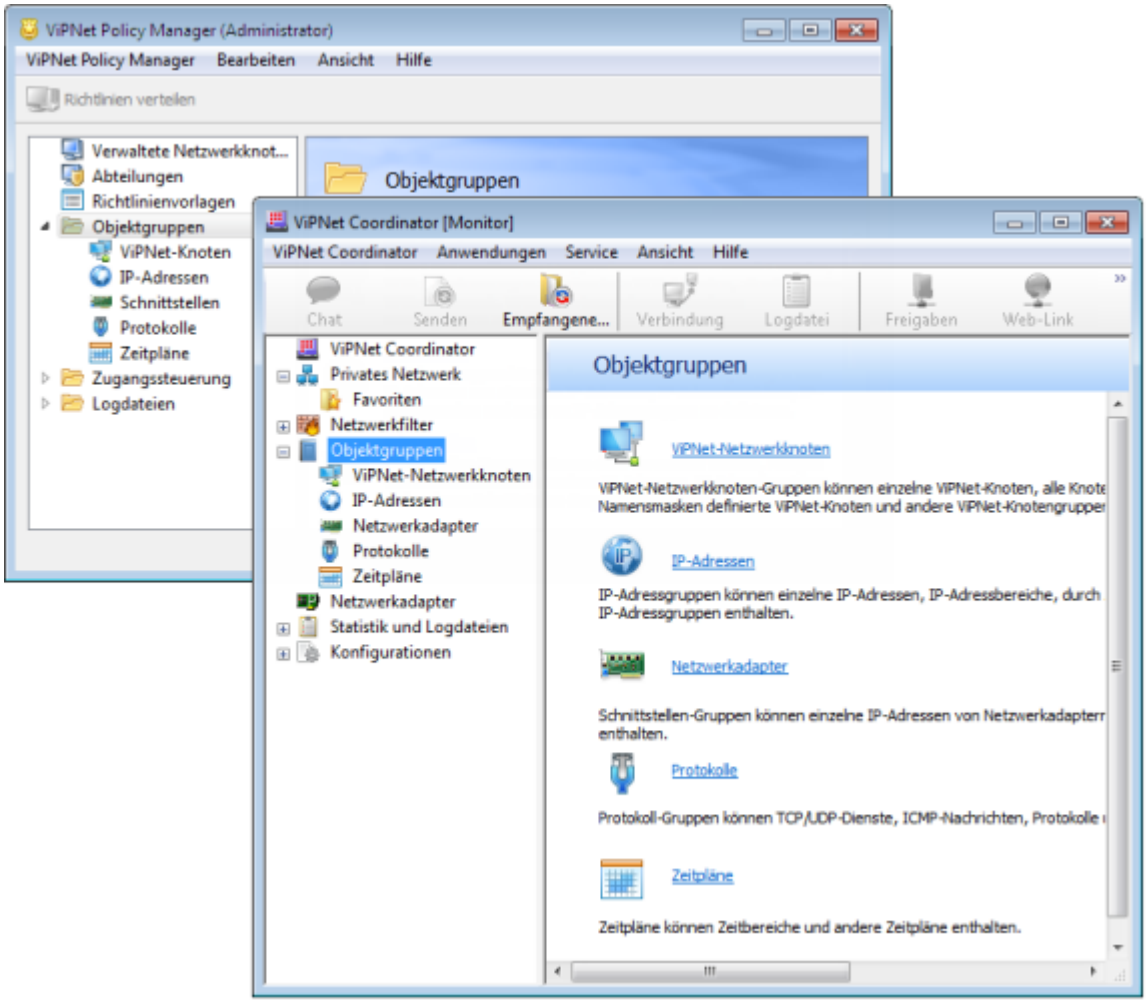

Abbildung 31. Objektgruppen in den Programmen ViPNet Monitor und ViPNet Policy Manager

Es gibt folgende Arten von Objektgruppen:

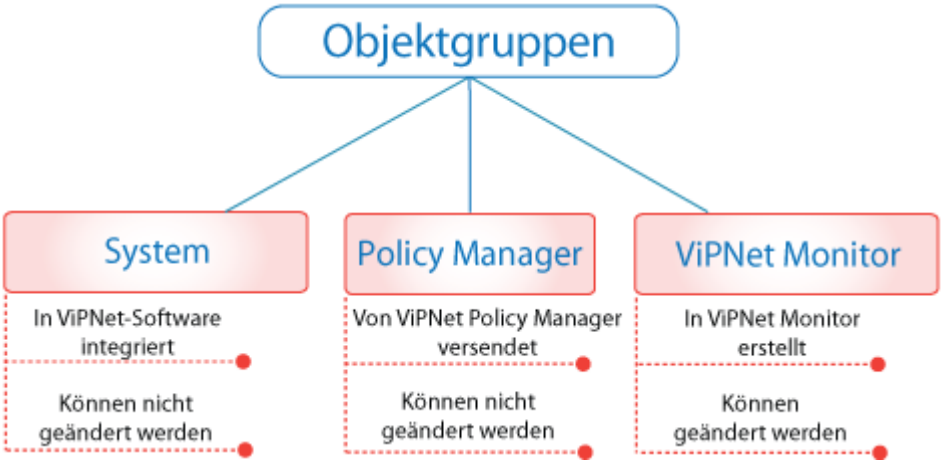

Abbildung 32. Typen von Objektgruppen

- System-Objektgruppen (auf S. 39). Diese Gruppen sind in der Software ViPNet Policy Manager, ViPNet Client Monitor und ViPNet Coordinator Monitor integriert und können nicht geändert werden.
- Objektgruppen, die von den Benutzern des Programms ViPNet Policy Manager erstellt werden. Diese Gruppen werden zusammen mit den Sicherheitsrichtlinien versendet und können nicht auf dem Netzwerkknoten geändert werden.
- Objektgruppen, die von den Benutzern der Programme ViPNet Client Monitor und ViPNet Coordinator Monitor erstellt werden, sowie einige standardmäßig definierte Objektgruppen. Diese Gruppen können vom Benutzer auf dem Netzwerkknoten geändert werden.

System-Objektgruppen

System-Objektgruppen repräsentieren in ViPNet Software integrierte Objektgruppen mit vorgegebenen Namen, die in Sicherheitsrichtlinienvorlagen und in benutzerdefinierten Objektgruppen verwendet werden können. Jede System-Objektgruppe besitzt ihren eigenen Anwendungsbereich.

Hinweis. System-Objektgruppen können nicht geändert oder gelöscht werden.

Jede System-Objektgruppe besitzt einen eigenen Anwendungsbereich:

1. Gruppe **Alle Clients** enthält alle Clients aus der Adressliste des Knotens.
2. Gruppe **Alle Coordinatoren** enthält alle Coordinatoren aus der Adressliste des Knotens.
3. Gruppe **Alle Objekte** enthält alle Objekte bestimmten Typs; wird nur als Bestandteil von Objektgruppen verwendet und dient dazu, Gruppen zu erstellen, die alle Objekte mit nur wenigen Ausnahmen umfassen.
4. Gruppe **Broadcast-Adressen** enthält Alle Broadcast-Adressen und wird beim Erstellen von Broadcast-Filtern verwendet.

5 Gruppe **Mein Knoten** enthält Eigener Knoten. Diese Gruppe kann nur als Quelle der IP-Pakete angegeben werden. In diesem Fall wird der Filter auch auf ausgehende Verbindungen des Knotens angewendet.

6 Gruppe **Andere Knoten** enthält andere Netzwerkknoten (alle Knoten mit Ausnahme des eigenen). Diese Gruppe kann nur als Quelle der IP-Pakete angegeben werden. In diesem Fall wird der Filter auch auf eingehende Verbindungen des Knotens angewendet.

7 Gruppe **Getunnelte Adressen** enthält alle IP-Adressen, die vom Coordinator-Knoten getunnelt werden.

8 Gruppe **Gruppenadressen** enthält Adressbereich für den Gruppenversand (224.x.0.0–239.255.255.255). Diese Gruppe kann nur als Ziel für offene Verbindungen angegeben werden.

Benutzer-Objektgruppen

Benutzer-Objektgruppen repräsentieren Gruppen von Objekten, die von Benutzern der Programme ViPNet Policy Manager und ViPNet Monitor für bestimmte Zwecke definiert werden. Die Namen der zu erstellenden Objektgruppen sollten eindeutig sein und sich von den Namen der System-Objektgruppen unterscheiden.

Es werden folgende Typen von Objektgruppen unterstützt:

- **ViPNet Netzwerkknoten**: Gruppe von Knoten im geschützten Netzwerk. Wird in Filtern des geschützten Netzwerks und der getunnelten Knoten verwendet. Standardmäßig sind die Gruppen **Öffentliche IP-Adressen** und **Private IP-Adressen** vorgegeben.
- **IP-Adressen**: eine beliebige Kombination einzelner IP-Adressen und IP-Adressbereiche oder DNS-Namen. Wird in NAT-Regeln und Netzwerkfiltern verwendet (mit Ausnahme der Filter des privaten Netzwerks).
- **Netzwerkadapter**: eine beliebige Kombination einzelner Netzwerkadapter oder IP-Adressen der Netzwerkadapter. Wird in Netzwerkfiltern auf Coordinatoren verwendet (mit Ausnahme der Filter des privaten Netzwerks)
- **Protokolle**: eine beliebige Kombination von Protokollen und Ports. Wird in allen Filtern und NAT-Regeln verwendet. Standardmäßig enthält diese Gruppe eine große Anzahl der am häufigsten verwendeten Protokolle.
- **Zeitpläne**: eine beliebige Kombination von Anwendungsregeln für Netzwerkfilter gemäß Uhrzeit und Wochentag. Wird in allen Filtern verwendet. Standardmäßig sind die Gruppen **Arbeitswoche** und **Ruhetage** vorgegeben.

Standardparameter der integrierten Firewall

Nun sind standardmäßig auf den Clients und Coordinatoren allerdings die Netzwerkfilter eingestellt, die den gesamten offenen Traffic durchlassen, d.h. die integrierte Firewall ist inaktiv. Das beugt Konfliktsituationen und Internetzugangsstörungen vor, im Falle wenn auf dem Knoten andere Firewalls aktiv sind (z.B. die Windows Firewall).

Wenn Sie den unerwünschten Traffic blockieren möchten, können Sie in den Programmen ViPNet Client und ViPNet Coordinator entsprechende Netzwerkfilter einrichten. Um die Firewalls auf den Knoten Ihres Netzwerks zentral verwalten zu können, wird der Einsatz des Programms ViPNet Policy Manager empfohlen.

Wenn Sie ein erfahrener Netzwerkadministrator sind, können Sie umgekehrt vorgehen, indem Sie alle offenen Verbindungen blockieren und nur den erwünschen Traffic erlauben. Dabei sollen Sie alle anderen Firewalls (einschließlich der Windows Firewall) deaktivieren.

Sicherheitsstufen

In den Programmen ViPNet Client und ViPNet Coordinator 3.2.x sind fünf Sicherheitsstufen vorgesehen. Jede dieser Sicherheitsstufen stellt eine Zusammensetzung von Regeln zur Verarbeitung offener IP-Pakete dar.

In Version 4.x werden Sicherheitsstufen nicht mehr verwendet. Das erforderliche Sicherheitsausmaß wird durch Definition entsprechender Filter an den betroffenen Netzwerkknoten erreicht. Beispiele für die Konfiguration sind in der unteren Tabelle aufgeführt.

Tabelle 4. Gegenüberstellung von Sicherheitsstufen der Version 3.2.x und Filtern der Version 4.x

Sicherheitsstufe	**Überschrift**
1 Alle Verbindungen blockieren	Löschen Sie im Bereich **Lokale Filter des offnen Netzwerks** (auf dem Coordinator) bzw. **Filter des offenen Netzwerks** (auf dem Client) den erlaubenden Filter für alle IP-Adressen.
2 Nur erlaubte Verbindungen durchlassen	Löschen Sie im Bereich **Lokale Filter des offenen Netzwerks** (auf dem Coordinator) bzw. **Filter des offenen Netzwerks** (auf dem Client) den erlaubenden Filter für alle IP-Adressen. Erstellen Sie die benötigten erlaubenden Filter.
3 Ausgehende Verbindungen erlauben außer verbotene	Erstellen Sie die erforderlichen blockierenden Filter und stellen Sie für diese Filter eine höhere Priorität als die Priorität der vorinstallierten erlaubenden Filter ein.
4 Alle Verbindungen erlauben	Die vorinstallierten erlaubenden Filter bleiben wirksam.
5 Alle IP-Pakete ohne Bearbeitung durchlassen	Deaktivieren Sie den Schutz des IP-Traffics (Menü **Datei** > **Konfigurationen** > **Schutz deaktivieren**).

Antispoofing

Damit innerhalb des Netzwerks ein hohes Ausmaß an Sicherheit gewährleistet werden kann, sollte auf dem Coordinator die Funktion des Antispoofing aktiviert werden. Im Programm ViPNet Coordinator der Version 3.2.x sollte dementsprechend eine Konfiguration des Antispoofing manuell durchgeführt werden.

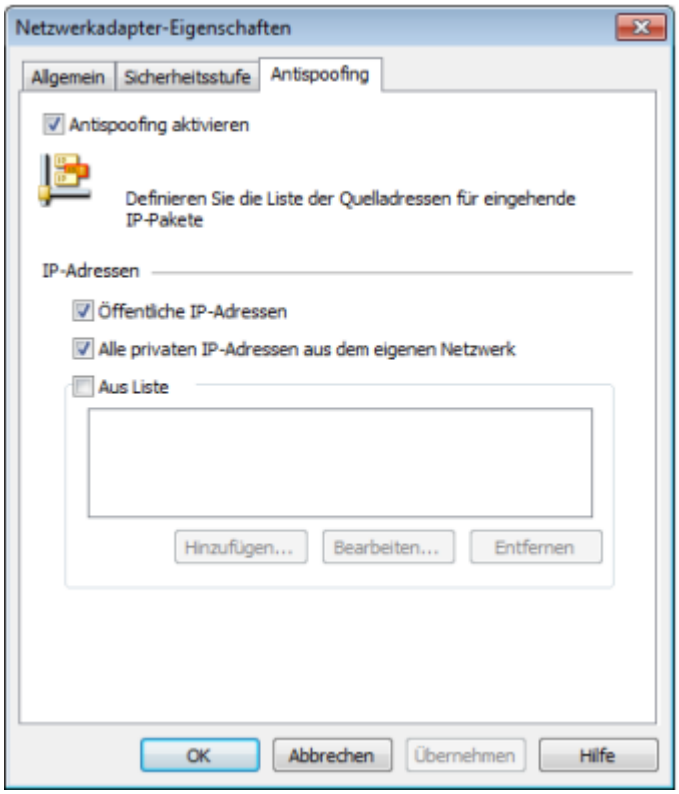

Abbildung 33. Aktivierung der Antispoofing-Funktion in der Version 3.2.x

In Version 4.x muss Antispoofing nicht mehr konfiguriert werden. Beim Aktivieren der Antispoofing-Funktion werden die entsprechenden Filter automatisch anhand der Routingtabelle des gegebenen Netzwerkknotens erstellt.

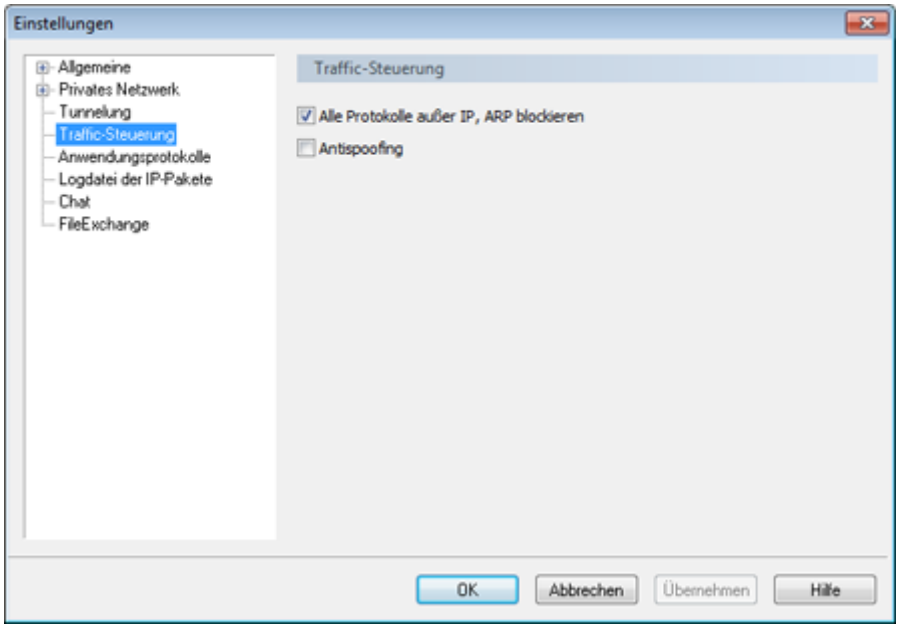

Abbildung 34. Antispoofing in der Version 4.x aktivieren

Konfiguration der Netzwerkadapterparameter

Im Programm ViPNet Coordinator Monitor Version 3.2.x können die Parameter der Netzwerkadapter im Bereich **Netzwerkadapter** konfiguriert werden: es können die Aliase der Netzwerkadapter, die Sicherheitsstufe und die Parameter für die Weiterleitung oder Blockierung der IP-Pakete (Antispoofing) definiert werden. In Version 4.x wird im Bereich **Netzwerkadapter** lediglich die Liste der Netzwerkadapter auf dem gegebenen Computer angezeigt. Zum Einstellen der benötigten Sicherheitsstufe (s. Sicherheitsstufen auf S. 41) müssen entsprechende Filter erstellt und den betroffenen Netzwerkadaptern zugewiesen werden.

Sperre des Computers und IP-Traffics

In ViPNet Monitor der Version 4.x wurde die Schaltfläche zur Sperre des Computers im Hauptfenster des Programms entfernt. Die Sperre des Computers wird nun mit Hilfe von Standardwerkzeugen des Betriebssystems ausgeführt.

Mit Hilfe des Programms ViPNet Monitor Version 4.x können Sie den gesamten IP-Traffic des Computers sperren. In diesem Fall werden alle Verbindungen mit geschützten oder offenen Knoten blockiert.

Sie können, wenn nötig, den Traffic-Schutz deaktivieren. In diesem Fall wird jede Verarbeitung des Traffics und die Protokollierung der Pakete in der Logdatei der registrierten IP-Pakete deaktiviert. Das Herstellen von Verbindungen zu geschützten ViPNet Knoten wird nicht mehr möglich sein.

Um den IP-Trafficschutz zu sperren oder deaktivieren, wählen Sie die entsprechende Optionen (**Schutz deaktivieren** oder **IP-Traffic sperren** im Menü **Datei** > **Konfigurationen**).

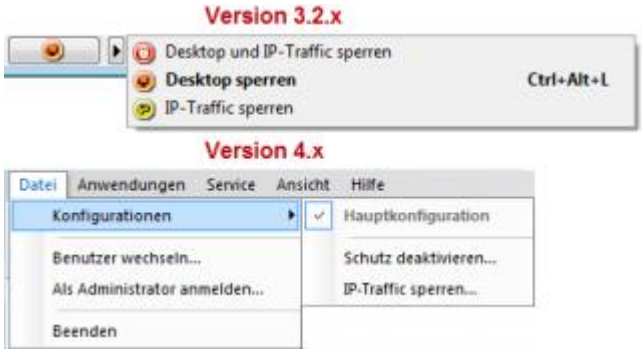

Abbildung 35. Konfiguration der Sperre des Computers und IP-Traffics

Beachten Sie auch, dass es im Konfigurationsfenster des Administrators keine Möglichkeit mehr gibt, den IP-Traffic beim Trennen des Authentisierungsgeräts zu sperren. Diese Option wurde entfernt, um die Prozedur der IP-Trafficsperre zu vereinfachen. Aktivieren Sie die Trafficsperre, wenn nötig, manuell.

Beim Arbeiten mit Netzwerkknoten-Administratorrechten in den Versionen 3.2.x und 4.x konnte die automatische Sperre des Computers bei längerer Inaktivität des Benutzers oder beim Trennen des Authentisierungsgeräts konfiguriert werden. Aus praktischen Gründen wurde die Konfiguration der Computersperre in Version 4.x überarbeitet.

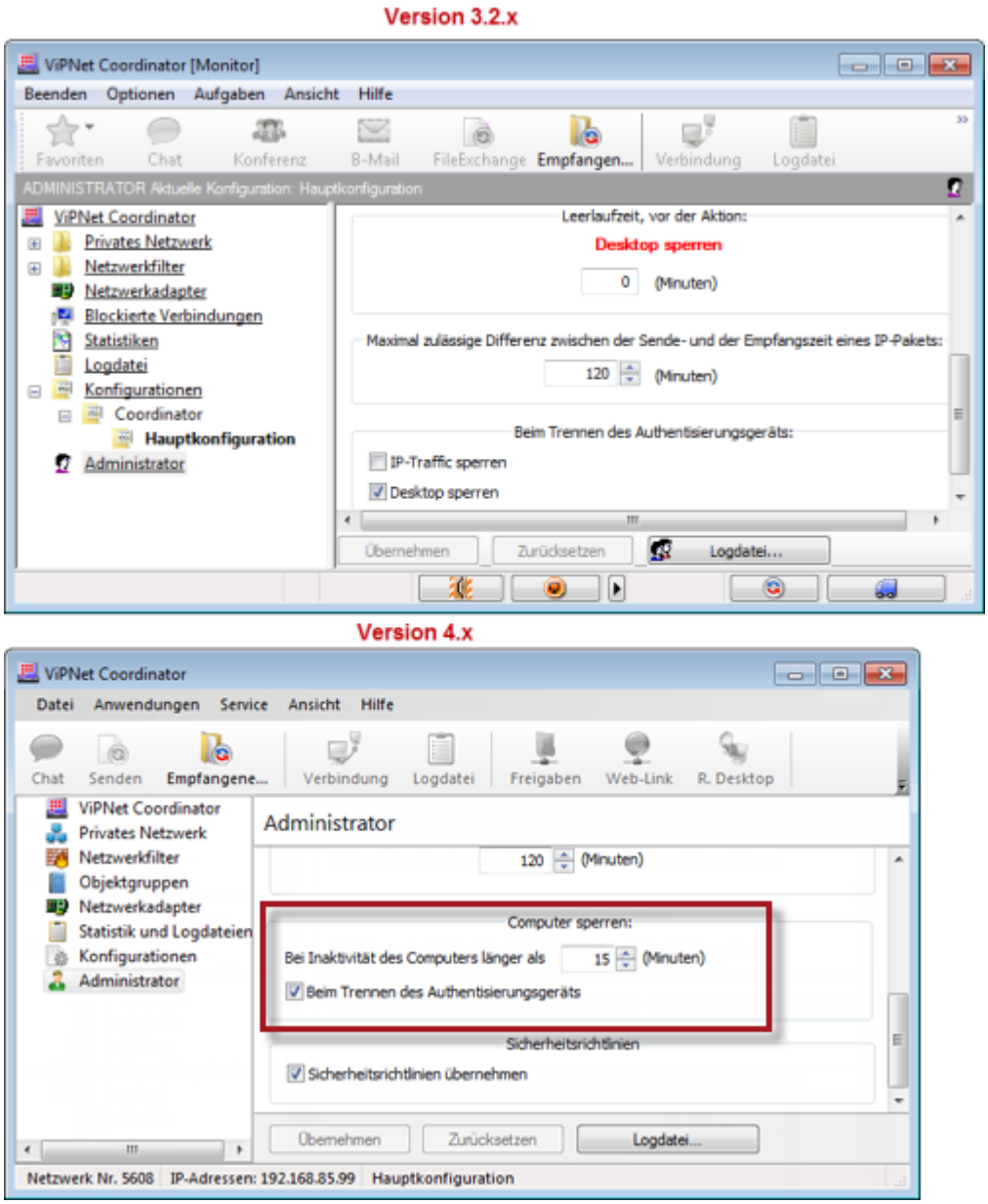

Abbildung 36. Sperre des Computers und IP-Traffics beim Arbeiten als Administrator

Benachrichtigung über Änderungen der Objektgruppen, Netzwerkfilter oder NAT-Regeln

In der neuen Version wird beim Hinzufügen oder Ändern von Objektgruppen, Netzwerkfiltern oder NAT-Regeln im Hauptfenster des Programms in der Statusleiste eine Meldung eingeblendet, dass die gegebenen Objekte geändert, jedoch noch nicht übernommen wurden. Die Meldung wird so lange angezeigt, bis die Schaltfläche Übernehmen gedrückt wird und der Benutzer innerhalb von 30 Sekunden bestätigt, dass die Änderungen übernommen werden.

In der Software ViPNet Client steht diese Möglichkeit nur im Administratormodus zur Verfügung.

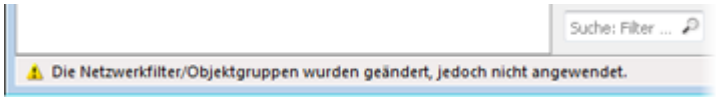

Abbildung 37. Benachrichtigung über Änderungen der Objektgruppen oder Netzwerkfilter

Anbindung an ViPNet Netzwerk

Konfiguration der Verbindung des Coordinators zum externen Netzwerk über eine Firewall mit statischem oder dynamischem NAT

Im Programm ViPNet Coordinator Monitor Version 3.2.x musste beim Konfigurieren der Verbindung des ViPNet Coordinators zum externen Netzwerk über eine Firewall mit statischem oder dynamischem NAT der Netzwerkadapter angegeben werden, über welchen die Verbindung aufgebaut wird (Liste **IP-Adresse des Netzwerkadapters, der unmittelbar mit der Firewall verbunden ist**).

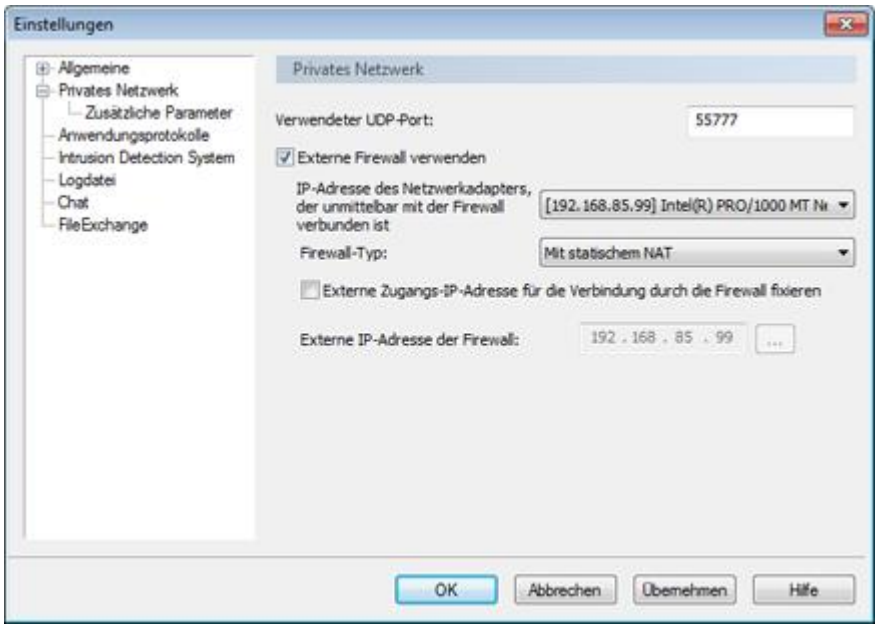

Abbildung 38. Konfiguration der Firewall mit statischem NAT in Version 3.2.x

In Version 4.x wurde diese Option aus Gründen der Benutzerfreundlichkeit entfernt. Der Netzwerkadapter wird beim Senden des IP-Pakets automatisch ermittelt. Nun sollte ein Netzwerkadapter nur dann angegeben werden, wenn Sie möchten, dass alle eingehenden IP-Pakete über eine bestimmte IP-Adresse der Firewall weitergeleitet werden. Bevor Sie den Adapter der Firewall angeben, sollten Sie das Kontrollkästchen **Externe Zugangs-IP-Adresse für die Verbindung durch die Firewall fixieren** aktivieren.

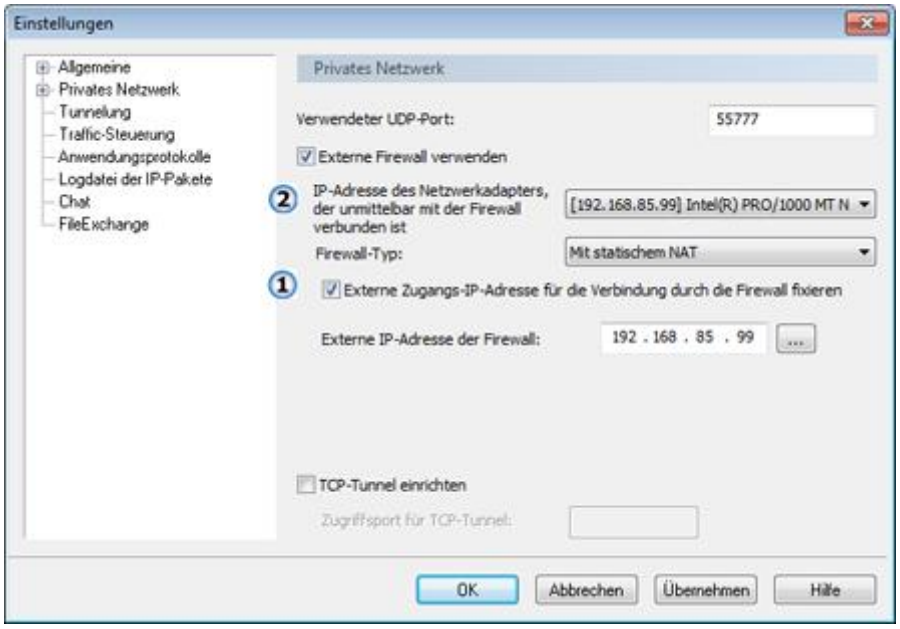

Abbildung 39. Festlegen des Firewall-Adapters in Version 4.x

Konfiguration der Clientverbindung zum ViPNet Netzwerk

In der neuen Programmversion von ViPNet Client wurde die Konfiguration der Verbindung des Clients mit einem externen Netzwerk vereinfacht. Früher mussten beim Konfigurieren der Verbindung der IP-Adressenserver und die Parameter der Firewall definiert werden. Nun sind für eine erfolgreiche Verbindung der Clients mit dem Netzwerk im Regelfall keine Einstellungen nötig. In besonderen Fällen kann die Änderung des Coordinators, der für den gegebenen Client als Verbindungsserver auftritt, erforderlich sein.

Diese Möglichkeit ist nur im Administratormodus zur Verfügung.

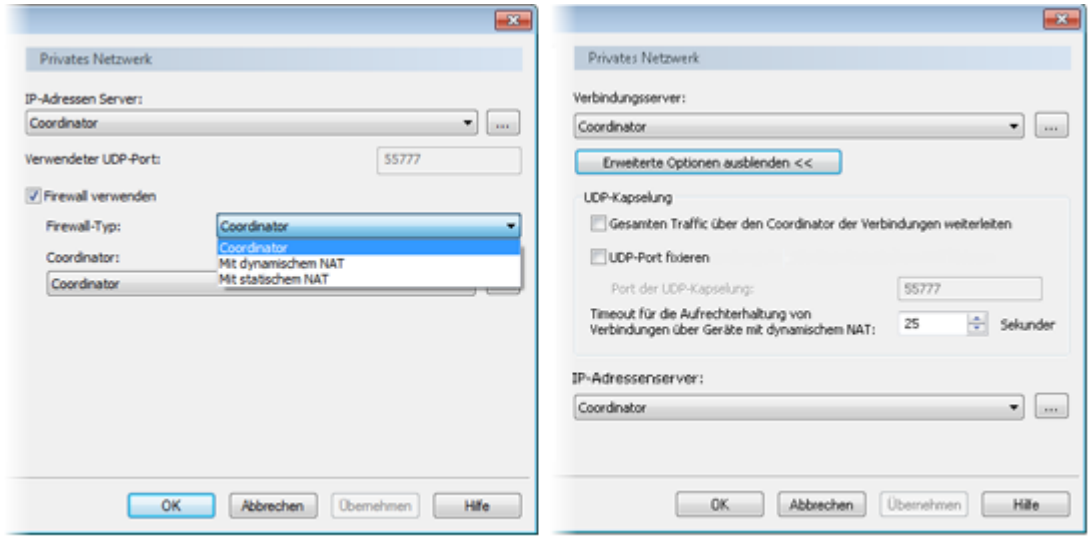

Abbildung 40. Änderung der Verbindungseinstellungen für das ViPNet-Netzwerk in ViPNet Client

Verbindung der Clients zum ViPNet Netzwerk über einen TCP-Tunnel

Bei Remoteverbindungen der Clients zum ViPNet Netzwerk kann ein Problem mit der Übermittlung der IP-Pakete über das UDP-Protokoll auftreten, da dieses Protokoll von einigen Serviceanbietern blockiert wird. Nun kann sich der Client über einen TCP-Tunnel, der auf seinem Verbindungsserver konfiguriert ist, mit den anderen ViPNet Netzwerkknoten verbinden. Der TCP-Tunnel wird dann verwendet, wenn eine Weiterleitung der IP-Pakete über das UDP-Protokoll nicht möglich ist.

Bei der Konfiguration des TCP-Tunnels auf dem Coordinator wird der Port angegeben, auf welchem die übermittelten TCP-Pakete eintreffen sollen. Es sollte beachtet werden, dass ein TCP-Tunnel nur auf einem Coordinator eingerichtet werden kann, der sich nicht hinter einer Firewall befindet oder hinter einer Firewall mit statischem NAT befindet.

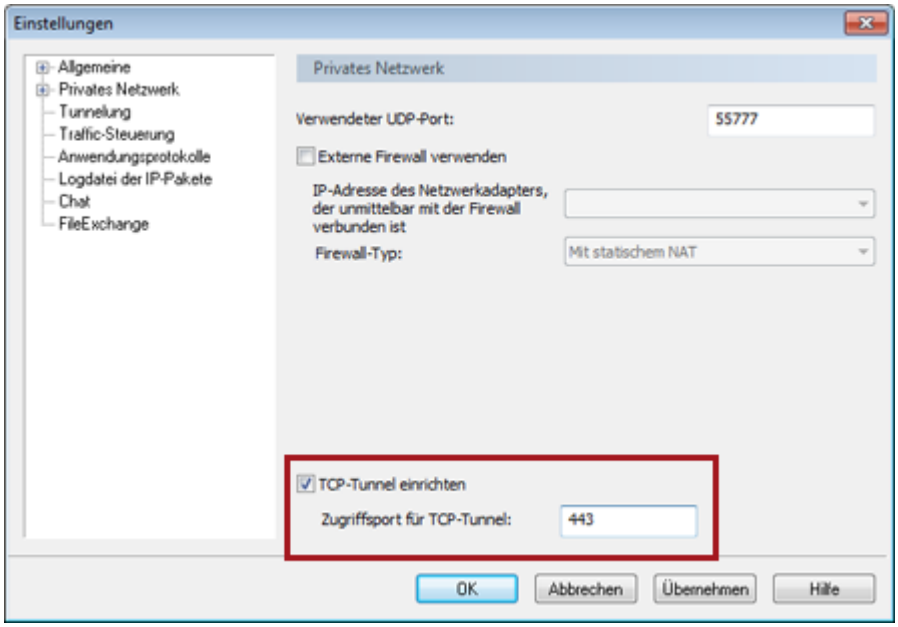

Abbildung 41. Einrichten des TCP-Tunnels in ViPNet Coordinator

Die Informationen über die Portnummer des TCP-Tunnels werden automatisch an alle Clients versendet, für welche der gegebene Coordinator als Verbindungsserver auftritt. Wenn ein Remoteclient im Weiteren nicht in der Lage ist, eine Verbindung zu den anderen ViPNet Netzwerkknoten über das UDP-Protokoll herzustellen, dann beginnt dieser Client automatisch, die benötigten Verbindungen über den TCP-Tunnel aufzubauen, der auf seinem Verbindungsserver konfiguriert ist. Die erhaltenen IP-Pakete werden auf dem Coordinator aus dem TCP-Tunnel extrahiert und an die Zielknoten über das UDP-Protokoll weitergeleitet.

Auf dem Client wird die Portnummer für den Zugang zum Coordinator über den TCP-Tunnel in den Eigenschaften dieses Coordinators angezeigt. Wenn die Portnummer nicht in den Coordinatoreigenschaften angegeben ist, und wenn gleichzeitig bekannt ist, dass ein TCP-Tunnel auf diesem Coordinator eingerichtet ist, dann kann die Portnummer manuell angegeben werden.

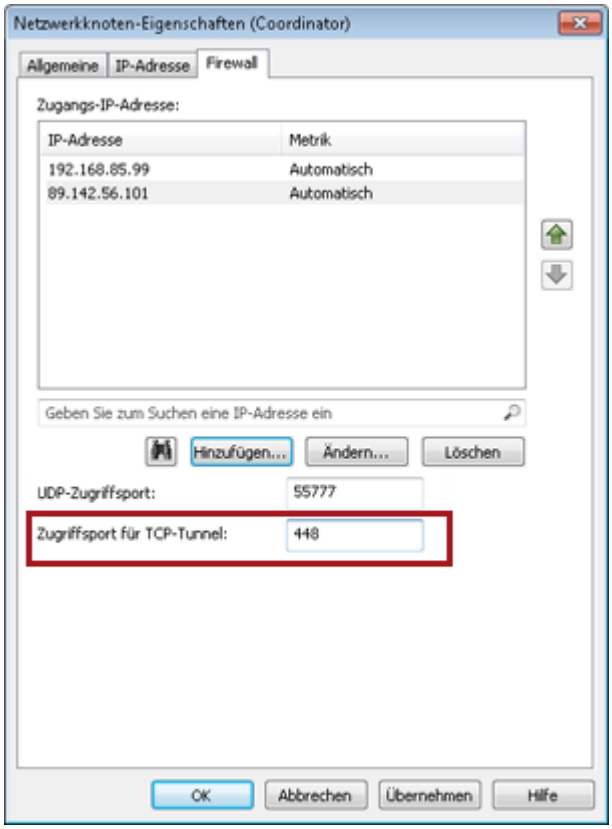

Abbildung 42. Definition des Zugangsports für den TCP-Tunnel

Sonstige Änderungen

Verwendung des Programms ViPNet Client mit vereinfachter Oberfläche

Früher wurde das Programm ViPNet Client mit seiner vollständigen Benutzeroberfläche auf den Netzwerkclients verwendet. Eine hohe Anzahl an Funktionen und Einstellungen des Programms konnte zu Schwierigkeiten auf Seiten der Benutzer führen. Nun wird auf den Clients das Programm ViPNet Client mit einer reduzierten Oberfläche verwendet. Mit Hilfe dieser Oberfläche kann der Benutzer mit der Liste der geschützten Knoten arbeiten, Nachrichten und Dateien mit anderen Benutzern austauschen und Updates der Adresslisten und Schlüssel annehmen. Alle Funktionen zur Konfiguration des Programms werden dabei vom Netzwerkknotenadministrator ausgeführt.

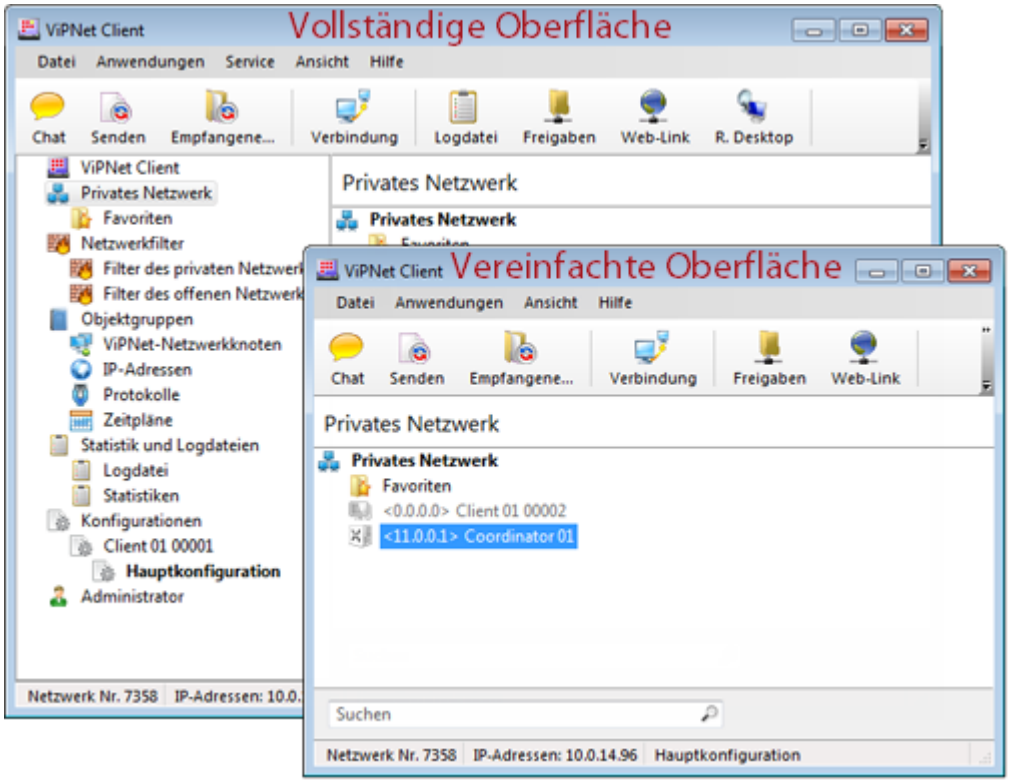

Abbildung 43. Benutzeroberfläche des Programms ViPNet Client Monitor

Authentisierungsmodus

Im Programm ViPNet Monitor der Version 4.x besteht die Möglichkeit, bei Verwendung eines Authentisierungsgeräts (Authentisierungsmodus **PIN und Authentisierungsgerät**) für die Anmeldung im Programm den Benutzer nicht nur mittels seines privaten Schlüssels (wie in Version 3.2.x), sondern auch mit Hilfe eines Zertifikats zu authentifizieren.

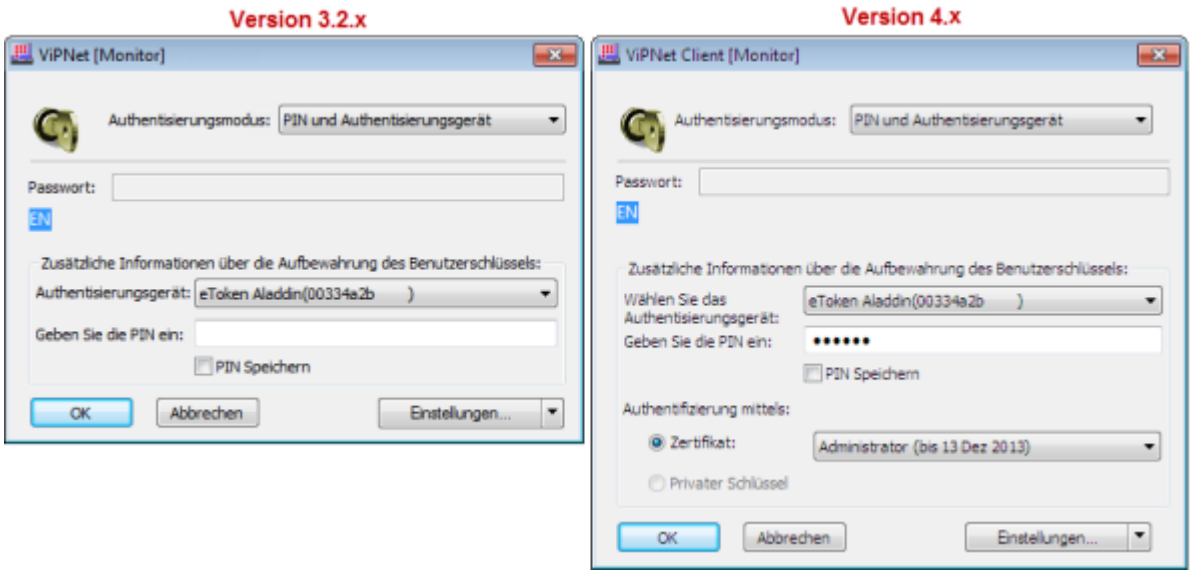

Abbildung 44. Verwendung eines Geräts für die Benutzer-Authentifizierung

Das für die Authentifizierung verwendete Zertifikat sollte von einer unbeteiligten Zertifizierungsstelle ausgestellt sein. Zusätzlich sollte auf dem Gerät ein privater, dem Zertifikat entsprechender Schlüssel gespeichert sein.

Für die Authentifizierung des Benutzers mit Hilfe eines Zertifikats sollten folgende Bedingungen erfüllt sein:

- Das externe Gerät sollte den Standard PKCS#11 inklusive der Funktionalität der digitalen Signatur und der Verschlüsselung unterstützen.
- Das Zertifikat sollte gültig sein (die Gültigkeitsdauer des Zertifikats sollte nicht abgelaufen sein).
- Das Zertifikat sollte nicht gesperrt sein.
- Die Zertifikatanwendung sollte „Echtheitsüberprüfung des Clients" lauten. Dieser Anwendungszweck wird im Fenster **Zertifikat**, in der Registerkarte **Eigenschaften**, im Feld **Erweiterte Schlüsselverwendung** angezeigt.
- Das Herausgeber-Zertifikat sollte im Systemspeicher **Vertrauenswürdige Stammzertifizierungsstelle** installiert sein.

Auf diese Weise können Sie für die Authentifizierung im Programm ViPNet Monitor das gleiche Gerät verwenden wie für die Authentifizierung in anderen Anwendungen und Systemen, was den hohen Bedienungskomfort und die einheitliche Verwendung des betroffenen Geräts gewährleistet.

Wenn im Programm ViPNet Monitor der Version 3.2.x der Authentisierungsmodus **Passwort auf Authentisierungsgerät** ausgewählt war, dann sollten Sie nach einem Update des Programms auf die Version 4.x den Authentisierungsmodus ändern. In nachfolgenden Versionen des Programms ViPNet Monitor wird der Authentisierungsmodus **Passwort auf Authentisierungsgerät** nicht mehr unterstützt.

Achtung! Beim Arbeiten im Programm ViPNet Monitor 4.x kann die Option **Passwort auf Authentisierungsgerät** nicht mehr vom Administrator des Netzwerkknotens ausgewählt werden. Dieser Modus kann nur dann weiter verwendet werden, wenn er bereits beim Arbeiten mit der Version 3.2.x ausgewählt war.

Der Authentisierungsmodus **Passwort auf Authentisierungsgerät** entspricht nicht mehr den Sicherheitsanforderungen und wird ausschließlich aus Gründen der Kompatibilität mit früheren Versionen der ViPNet Software unterstützt.

Wechsel der Programmkonfigurationen nach Zeitplan

Im Programm ViPNet Monitor Version 4.0 besteht die Möglichkeit, Programmkonfigurationen automatisch zu wechseln. Wenn Sie mit mehreren Programmkonfigurationen arbeiten, und jede dieser Konfigurationen zu einem bestimmten Zeitpunkt geladen werden soll, dann können Sie einen Zeitplan für den Wechsel der Konfigurationen einstellen. Die Konfiguration des Zeitplans und der Benachrichtigungen über den Konfigurationswechsel wird im Bereich **Konfigurationen** durchgeführt.

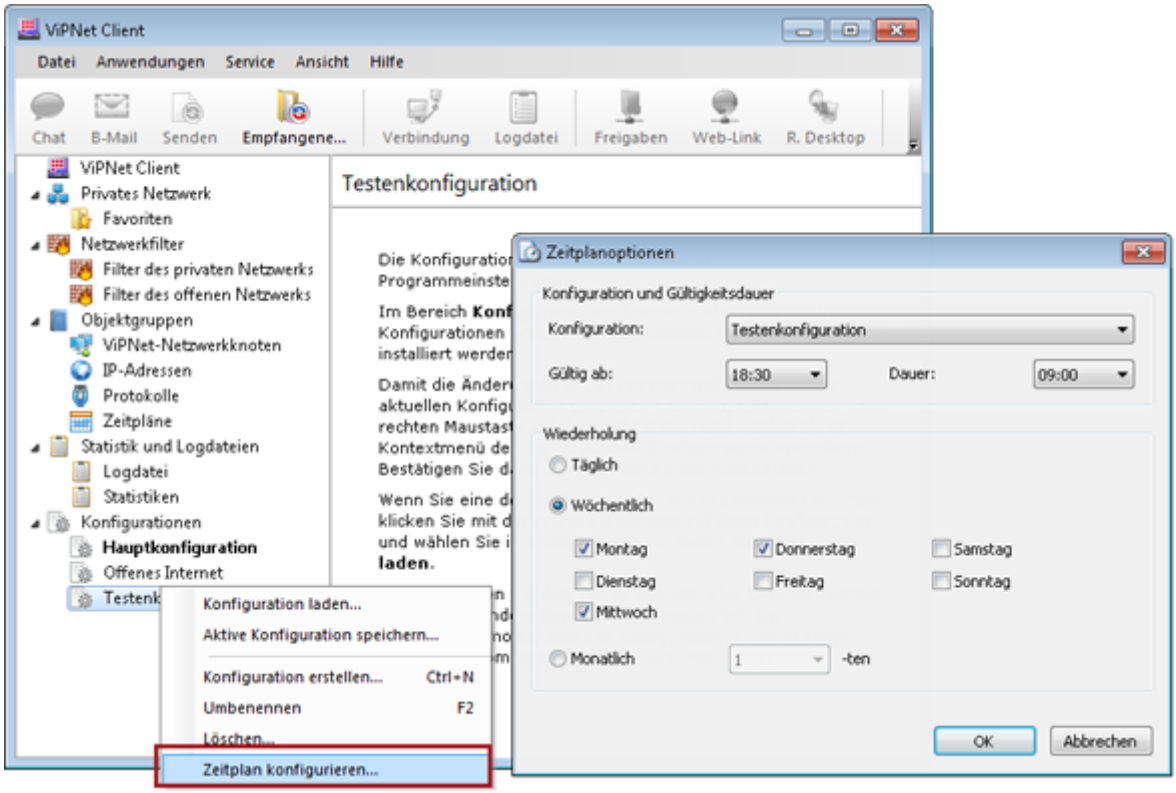

Abbildung 45. Erstellen eines Zeitplans für den Konfigurationswechsel

Änderungen im Programm ViPNet Business Mail

Im Programm ViPNet Business Mail Version 4.x wurden folgende Änderungen implementiert:

- Verwendung der integrierten Datenbank SQLite (s. Integrierte Datenbank SQLite auf S. 53);
- Speicherung der Anhänge in der Datenbank (s. Speicherung der Anhänge in der Datenbank und Archivierung auf S. 54);
- graphische Darstellung des Nachrichtenstatus (s. Anzeige des Nachrichtenstatus auf S. 54);
- Möglichkeit der Formatierung des Nachrichtentextes (auf S. 55);
- Hinzufügung neuer Autoprocessing-Regeln;
- Möglichkeit des Auswählen von Empfänger der Nachrichten und Entfernen der Signaturen beim Einstellen der Autoprocessing-Regeln für eingehende Nachrichten.

In der Benutzeroberfläche von ViPNet Business Mail werden ebenfalls neue Symbole verwendet.

Integrierte Datenbank SQLite

Im Programm ViPNet Business Mail Version 4.x wird die integrierte Datenbank SQLite verwendet. Die Konvertierung der Daten in das neue Format wird beim erstmaligen Start des Programms ViPNet Business Mail nach dem Update automatisch durchgeführt. Die Verwendung der SQLite-Datenbank hebt die Einschränkungen bezüglich der Anzahl der Nachrichten im Archiv auf (in Version 3.2.x konnten nicht

mehr als 120000 Nachrichten im Archiv gespeichert werden) und bietet die Möglichkeit zur gleichzeitigen Verarbeitung ein- und ausgehender Nachrichten beim Autoprocessing.

Speicherung der Anhänge in der Datenbank und Archivierung

In früheren Versionen von ViPNet Business Mail werden die Nachrichten getrennt von den Anhängen gespeichert. Beim Archivieren wird in diesem Fall ein Archiv erstellt, das eine Datei mit der Postdatenbank sowie eine Reihe von Ordnern enthält, in denen die Anhänge als gesonderte Dateien gespeichert werden. In Version 4.x besteht nun zusätzlich die Möglichkeit, die Anhänge in die Datenbank zu übertragen, um sie gemeinsam mit den Nachrichten zu archivieren. In diesem Fall besteht das Archiv nur aus einer Datei. Durch das gemeinsame Speichern von Nachrichten und Anhängen in einem Archiv kann das Kopieren oder Übertragen des Archivs auf einen externen Datenträger (z. B. für Backup-Zwecke) wesentlich vereinfacht werden.

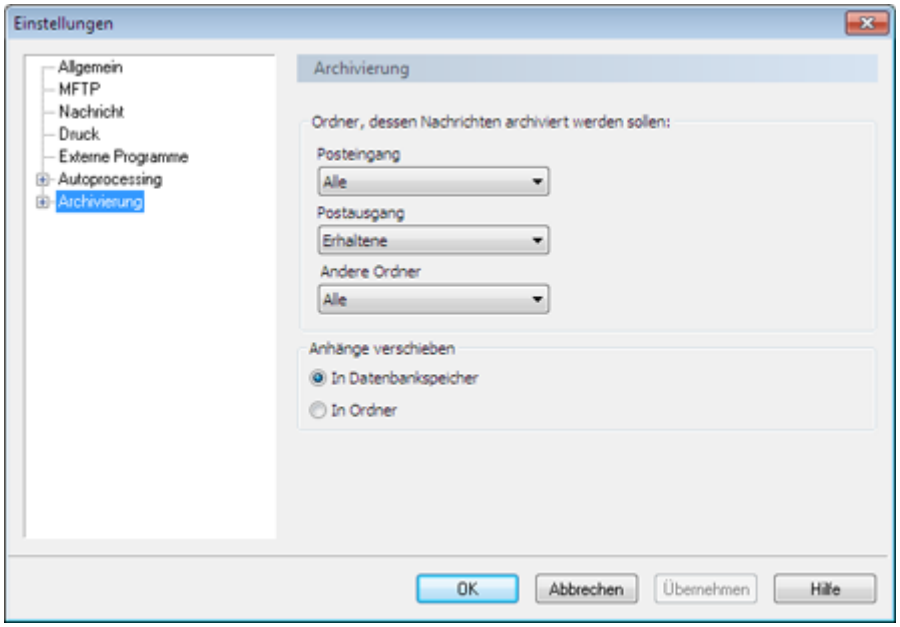

Abbildung 46. Konfiguration der Archivierung von Nachrichten und Anhängen

Anzeige des Nachrichtenstatus

Im Programm ViPNet Business Mail Version 4.x können Sie den für Sie passenden Anzeigemodus für die Nachrichtenstati auswählen: in Form von Buchstaben in der Spalte **Attribute** (diese Möglichkeit war bereits in den früheren Versionen implementiert) oder in graphischer Form in der neuen Spalte **Status**.

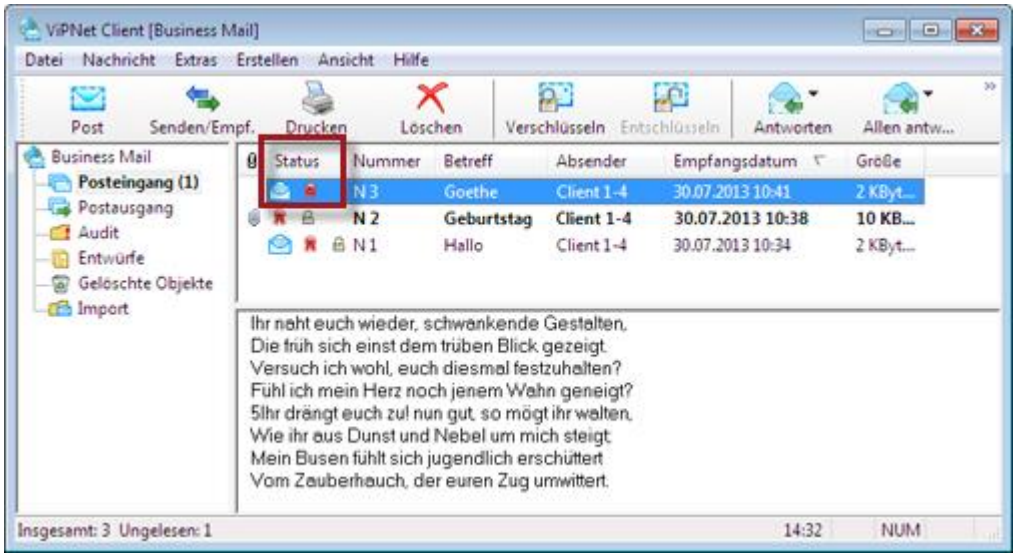
ViPNet Client [Business Mail]
Datei Nachricht Extras Erstellen Ansicht Hilfe
Post Senden/Empf. Drucken Löschen Verschlüsseln Entschlüsseln Antworten Allen antw...
Business Mail
Posteingang (1)
Postausgang
Audit
Entwürfe
Gelöschte Objekte
Import
Status Nummer Betreff Absender Empfangsdatum Größe
N 3 Goethe Client 1-4 30.07.2013 10:41 2 KByt...
N 2 Geburtstag Client 1-4 30.07.2013 10:38 10 KB...
N 1 Hallo Client 1-4 30.07.2013 10:34 2 KByt...
Ihr naht euch wieder, schwankende Gestalten,
Die früh sich einst dem trüben Blick gezeigt.
Versuch ich wohl, euch diesmal festzuhalten?
Fühl ich mein Herz noch jenem Wahn geneigt?
Ihr drängt euch zu! nun gut, so mögt ihr walten,
Wie ihr aus Dunst und Nebel um mich steigt;
Mein Busen fühlt sich jugendlich erschüttert
Vom Zauberhauch, der euren Zug umwittert.
Insgesamt: 3 Ungelesen: 1
14:32
NUM

Abbildung 47. Neue Spalte für die Anzeige des Nachrichtenstatus

Formatierung des Nachrichtentextes

In den früheren Versionen des Programms ViPNet Business Mail wurde die Formatierung des Nachrichtentextes nicht unterstützt. In der Version 4.x kann das Format der Nachrichten bei deren Erstellung konfiguriert werden, indem die Schriftart, die Schriftgröße und der Schriftschnitt geändert, ein Bild, eine Liste in den Text eingefügt werden usw. Dazu wird im Fenster zum Verfassen von Nachrichten die Textformatierungsleiste hinzugefügt.

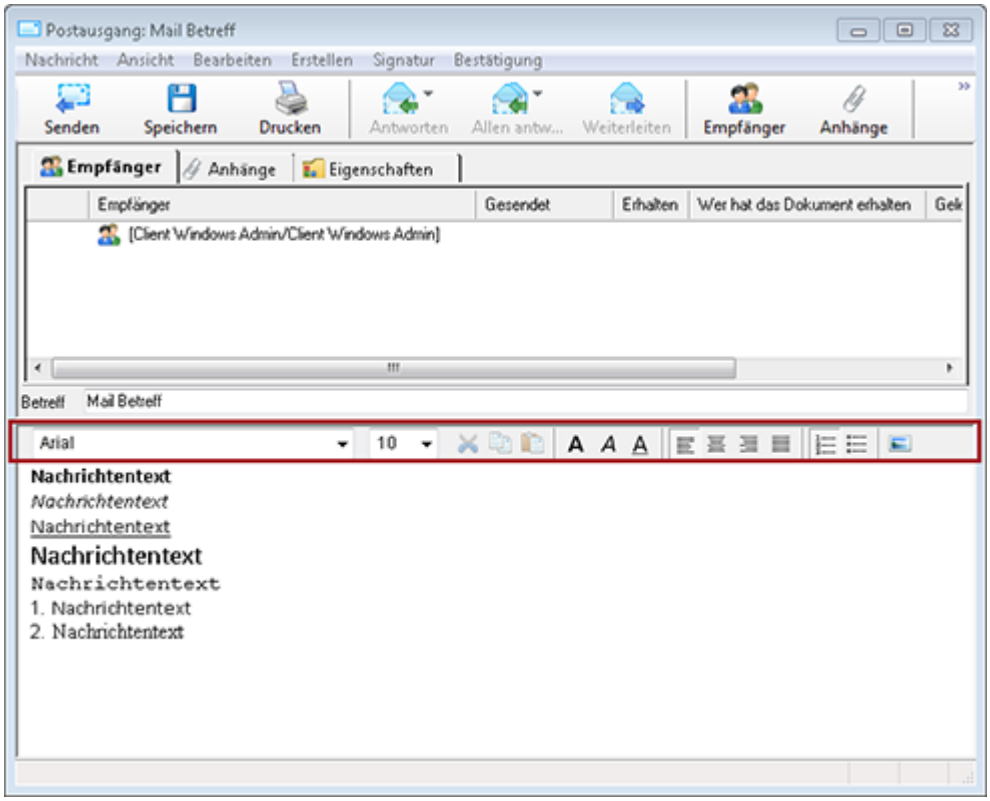

Abbildung 48. Änderungen in ViPNet Business Mail

Wollen Sie Nachrichten ohne Formatierung versenden, kann die Textformatierungsleiste ausgeblendet werden. Ändern Sie dazu die Einstellungen von allgemeinen Parametern.

Versenden Sie eine Nachricht mit Formatierung an den Empfänger, der eine frühere Version vom Programm ViPNet Business Mail verwendet, erhält dieser Empfänger Ihre Nachricht als Anhang, der den Text Ihrer Nachricht mit Formatierung enthält.

Hinzufügen von getunnelten Adressen

Wenn Sie im Programm ViPNet Monitor 3.2.x die IP-Adressen der getunnelten Knoten festlegen möchten, dann können Sie dazu im entsprechenden Bereich auf die Schaltfläche **Tunnelung** klicken und die Adressen hinzufügen. In Version 4.0 werden die IP-Adressen der getunnelten Knoten im Fenster der Eigenschaften des tunnelnden Coordinators im Bereich **Tunnelung** hinzugefügt. In diesem Bereich wird auch die erlaubte Anzahl an gleichzeitig getunnelten Knoten angezeigt.

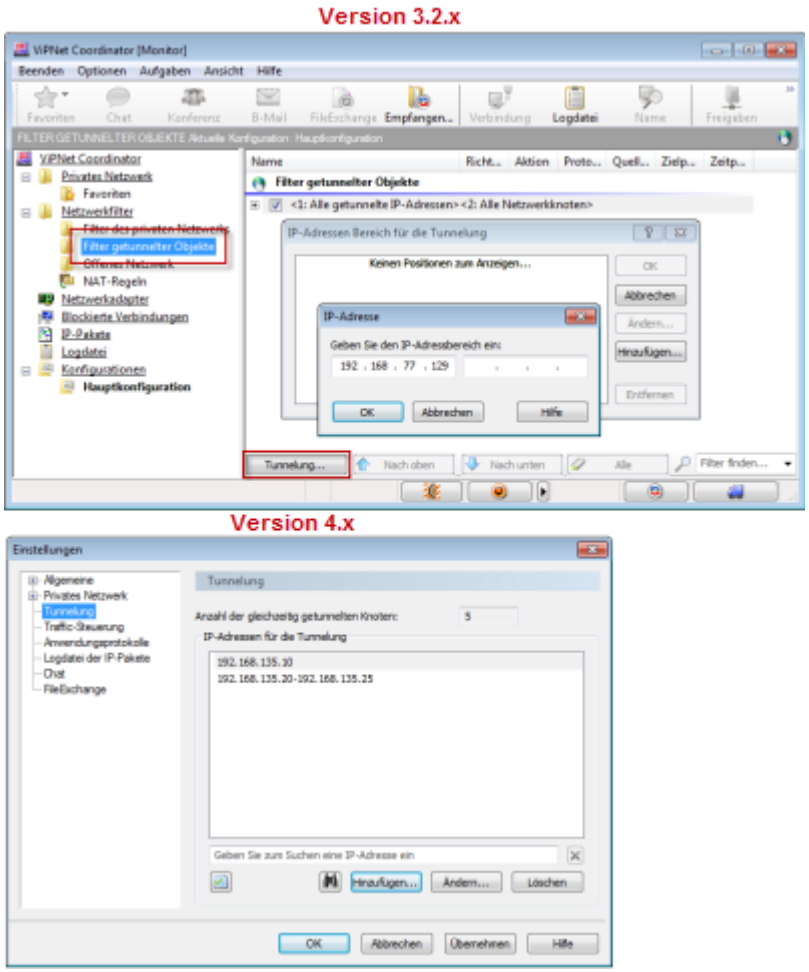

Abbildung 49. Festlegen von IP-Adressen der getunnelten Knoten

Ermitteln und Überprüfen von IP-Adressen

In Version 4.x können Sie beim Hinzufügen von IP-Adressen die IP-Adresse des Netzwerkknotens anhand des Computernamens ermitteln, indem Sie auf die Schaltfläche klicken.

In Version 3.2.x wird beim Hinzufügen einer IP-Adresse überprüft, ob es Überschneidungen zwischen den IP-Adressen in der Liste und den für andere Knoten des ViPNet Netzwerks angegebenen IP-Adressen gibt. Diese Überprüfung dient dazu, das Eintragen von identischen IP-Adressen zu vermeiden. Im Zuge der Überprüfung werden für den Benutzer Meldungen über alle IP-Adressenkonflikte angezeigt, die im ViPNet Netzwerk festgestellt wurden.

Beim Hinzufügen einer IP-Adresse in Version 4.x wird lediglich überprüft, ob sich die angegebene IP-Adresse mit den IP-Adressen in der Liste oder mit den IP-Adressen anderer Netzwerkknoten überschneidet. Wenn ein Konflikt festgestellt wird, dann erhält der Benutzer eine Meldung, die nur die neu angegebene IP-Adresse betrifft. Eine Überprüfung aller IP-Adressen in Version 4.x können Sie, wenn nötig, mit Hilfe der Schaltfläche starten.

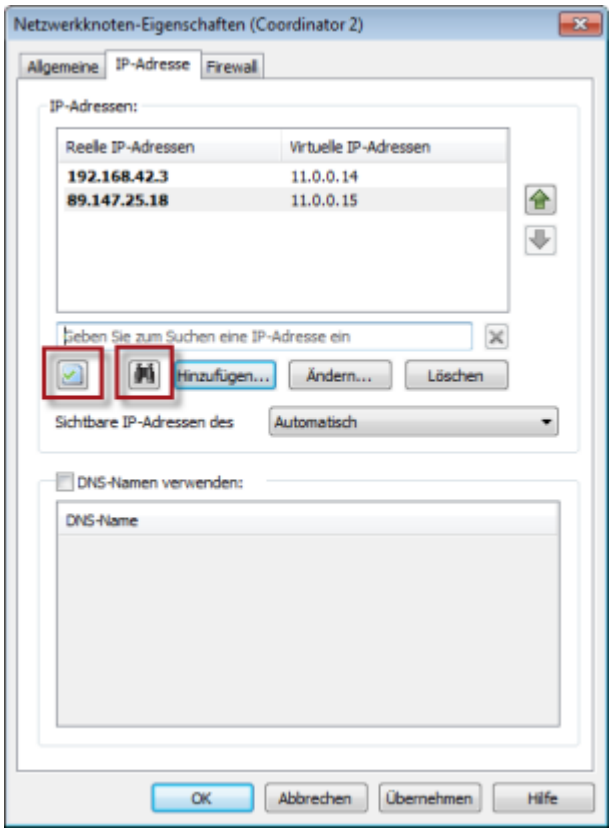

Abbildung 50. Hinzufügen und Überprüfen der IP-Adressen in Version 4.0

Logdatei der IP-Pakete

Im Programm ViPNet Monitor Version 3.2.x befindet sich die Logdatei der blockierten Verbindungen in einem separaten Bereich. In diesem Bereich können erlaubende Filterregeln auf Basis von Parametern der blockierten IP-Pakete erstellt werden.

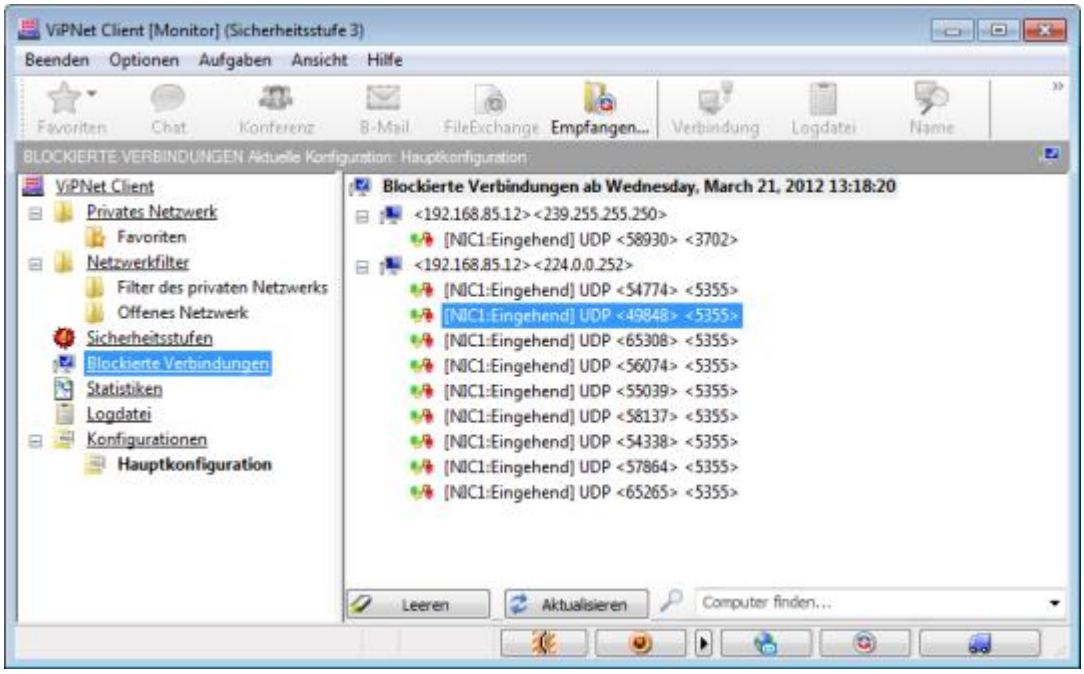

Abbildung 51. Liste der blockierten IP-Pakete

Im Programm ViPNet Monitor Version 4.x besteht die Möglichkeit, in der Logdatei der IP-Pakete sowohl erlaubende als auch blockierende Filter zu definieren. Alle Aktionen im Zusammenhang mit IP-Paketen können nun im Bereich **Logdatei der IP-Pakete** durchgeführt werden.

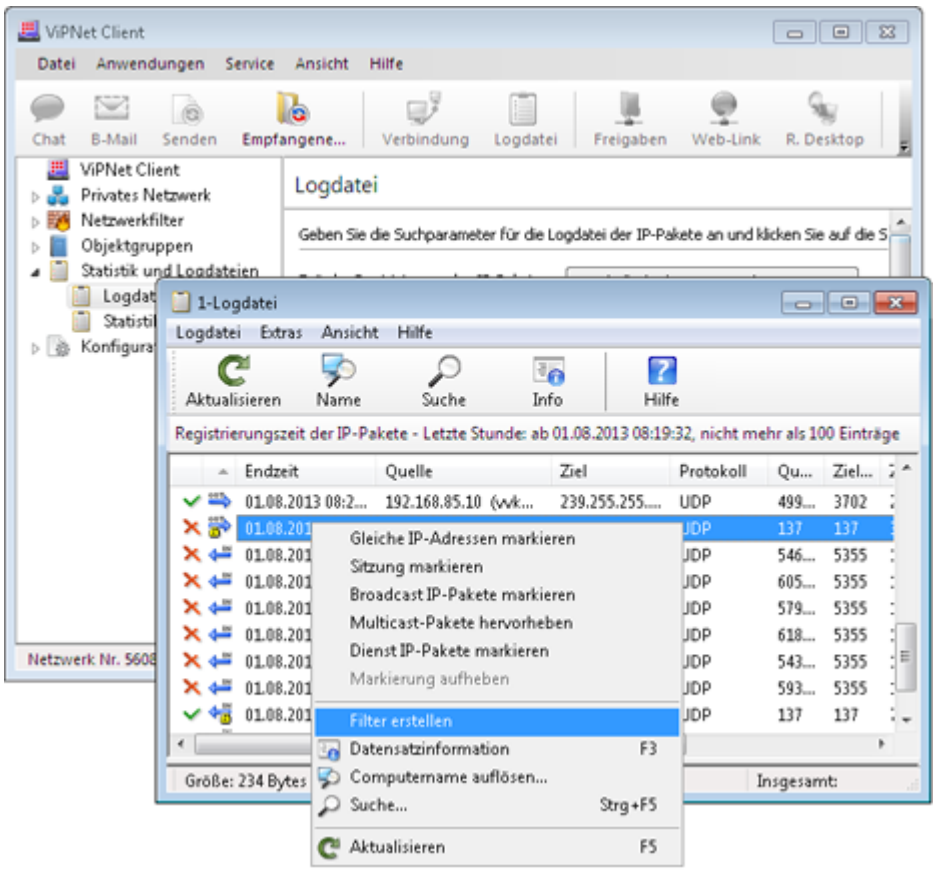

Abbildung 52. Logdatei der IP-Pakete in Version 4.x

Integration mit dem Programm SafeDisk-V

Im Programm ViPNet Monitor Version 3.2.x wurde die Möglichkeit zur gemeinsamen Verwendung mit dem Programm ViPNet SafeDisk-V 4.1 implementiert. Die Integration des Programms ViPNet Client Version 4.x mit dem Programm ViPNet SafeDisk-V Version 4.2 ist nun sichergestellt.

Der Grundsatz der Wechselwirkung der neuen Programmversionen von ViPNet SafeDisk-V und ViPNet Monitor hat sich geändert. Beim Starten von ViPNet SafeDisk-V steht ein Großteil der Einstellungen im Programm ViPNet Client Monitor nicht mehr für die Bearbeitung zur Verfügung. Es ist dann aus Sicherheitsgründen nicht mehr möglich, z. B. den Benutzer zu wechseln, den Schutz des IP-Traffics zu deaktivieren oder sich im Programm ViPNet Monitor abzumelden.

Anstelle von geschützten und ungeschützten Konfigurationen des Programms ViPNet Monitor werden nun automatisch zusätzliche Netzwerkfilter erstellt, die offene Verbindungen blockieren.

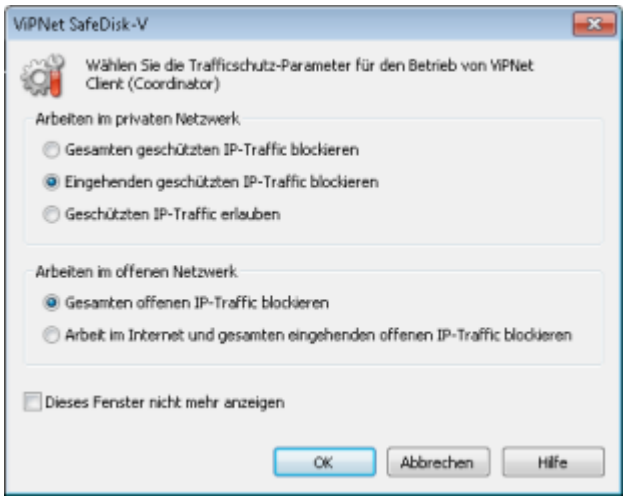
ViPNet SafeDisk-V
Wählen Sie die Trafficschutz-Parameter für den Betrieb von ViPNet Client (Coordinator)
Arbeiten im privaten Netzwerk
Gesamten geschützten IP-Traffic blockieren
Eingehenden geschützten IP-Traffic blockieren
Geschützten IP-Traffic erlauben
Arbeiten im offenen Netzwerk
Gesamten offenen IP-Traffic blockieren
Arbeit im Internet und gesamten eingehenden offenen IP-Traffic blockieren
Dieses Fenster nicht mehr anzeigen
OK
Abbrechen
Hilfe

Abbildung 53. Konfiguration der Trafficschutz-Parameter für

Übermitteln von MFTP-Dateien über Mailserver

In ViPNet Monitor 4.x besteht die Möglichkeit, die Dateien bei ihrer Übertragung über den SMTP/POP3-Kanal in Fragmente aufzuteilen. Diese Funktionalität ermöglicht es Ihnen, große Dateien auch dann zu versenden, wenn es auf dem Mailserver Einschränkungen für die maximale Größe der übermittelten Dateien gibt.

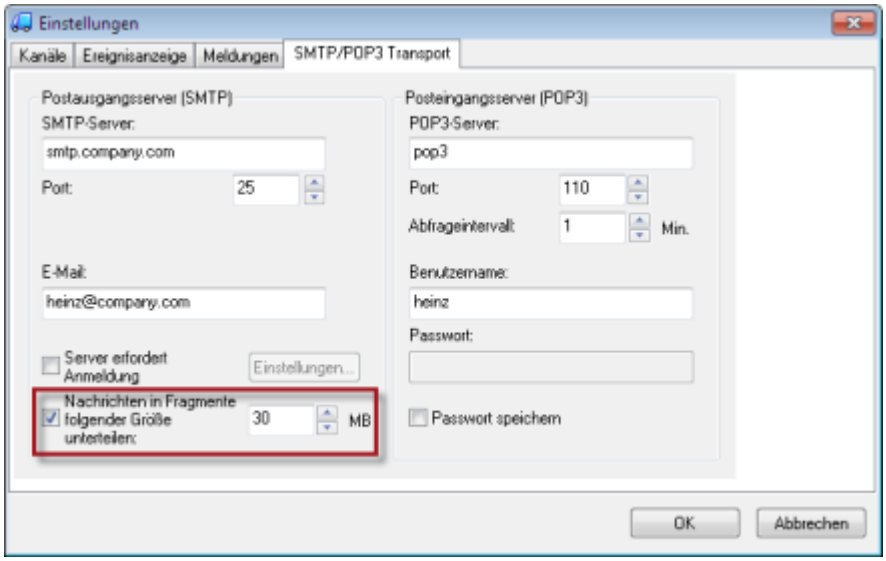

Abbildung 54. Konfiguration der Fragmentierung von Dateien

Neue Möglichkeiten im verschlüsselten Chat

Im Programm Verschlüsselter Chat der Version 4.2 stehen einige zusätzliche Features zur Verfügung. Nun können Sie folgende Aktionen durchführen:

- nach Wörtern in den Meldungen der aktuellen Chatsitzung suchen;
- zur vorhergehenden oder nächsten durchgesehenen Sitzung wechseln;
- Zeit und Datum der letzten Nachricht eines Sitzungsteilnehmers anzeigen;
- Dateien oder E-Mails während der Chatsitzung versenden.

  E-Mails können nur dann versendet werden, wenn die Software ViPNet Business Mail auf dem Client installiiert ist.

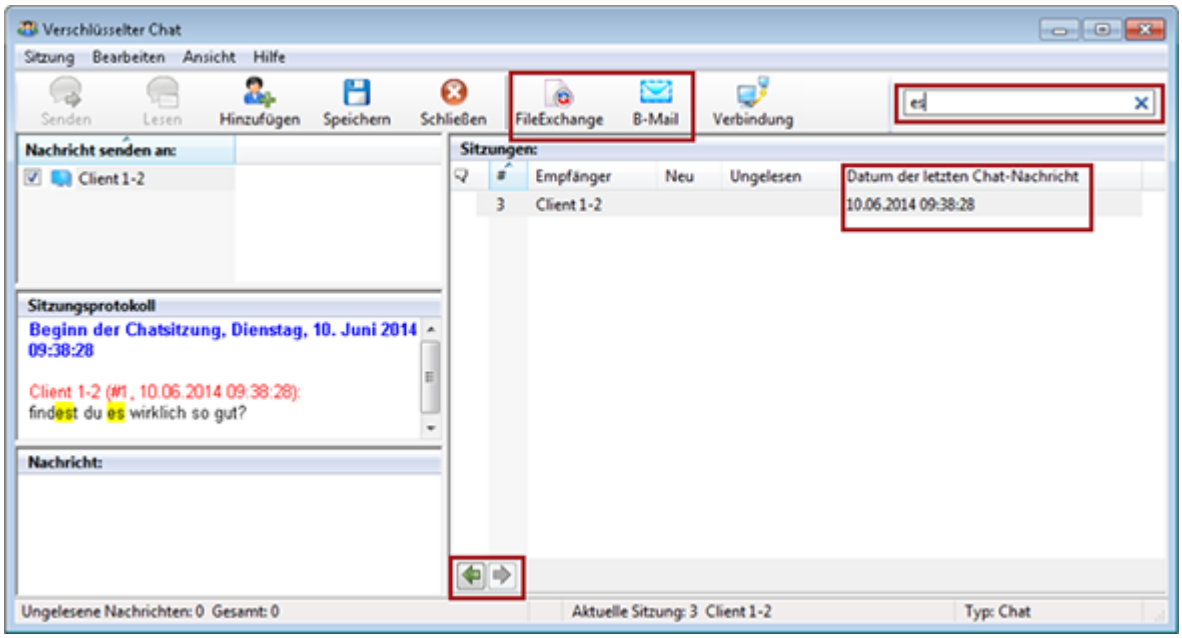

Abbildung 55. Neue Möglichkeiten im verschlüsselten Chat

Außerdem können Sie das Programm nun schließen, ohne vorher die Chatsitzungen zu beenden.

Änderungen der Benutzeroberfläche

Die Änderungen in der Arbeitsweise einiger Funktionen von ViPNet Monitor haben zu einer Überarbeitung der Benutzeroberfläche des Programms geführt. Alle Überarbeitungen zielen auf eine Vereinfachung der Arbeit mit dem Programm hin und sollen die Benutzerfreundlichkeit des Programms beim Arbeiten mit Netzwerkfiltern und NAT-Regeln, die vom ViPNet Policy Manager erhalten wurden, verbessern. Die wichtigsten Änderungen in der Benutzeroberfläche des Programms ViPNet Monitor werden weiter unten beschrieben.

Die Schaltflächen für den Aufruf der Programmkomponenten „Business Mail“, „Programmkontrolle“, „FileExchange“ und MFTP wurden aus der Statusleiste des Programmfensters von ViPNet Monitor entfernt. Der Wechsel zu einer dieser Komponenten oder zum Programm „Verschlüsselter Chat“ kann nun über das Menü Anwendungen erfolgen.

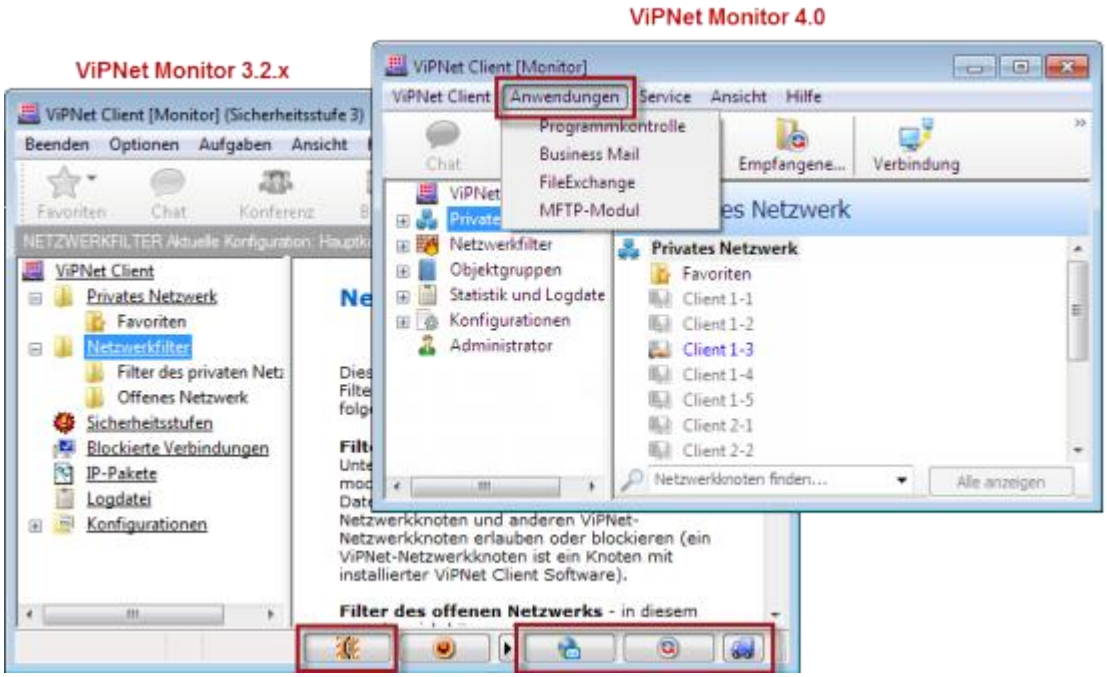

Abbildung 56. Wechsel zu einzelnen Komponenten der ViPNet-Software

In Version 4.x können Befehle für verbundene Netzwerkknoten, die früher im Menü **Aktionen** enthalten waren, nur noch aus dem Kontextmenü aufgerufen werden. Das Menü **Aktionen** wurde aus dem Hauptmenü entfernt.

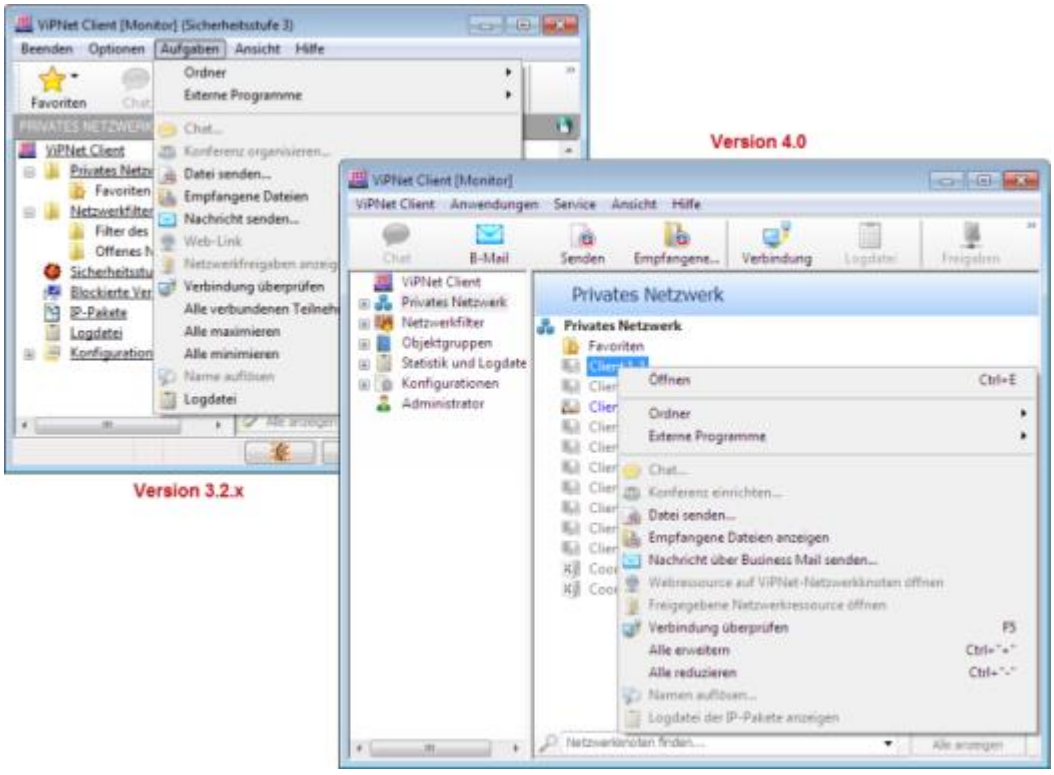

Abbildung 57. Mögliche Aktionen

Im Hauptfenster des Programms im Bereich **Privates Netzwerk** wird der eigene ViPNet Knoten nicht mehr angezeigt.

Die Schaltfläche für die Sperre des Computers (s. Sperre des Computers und IP-Traffics auf S. 43) wurde entfernt. In Version 4.x kann der Computer ausschließlich mit Hilfe der Standardwerkzeuge des Betriebssystems gesperrt werden.

Die Anzeige der Netzwerkfilter hat sich geändert. Aus Gründen der Übersichtlichkeit und um die Arbeit mit Netzwerkfiltern und NAT-Regeln einfacher zu gestalten, wurde die Anzeige der Filter in den Programmen ViPNet Monitor und ViPNet Policy Manager vereinheitlicht (s. Filterung des Traffics auf S. 27).

In Version 4.x werden die Konfiguration der Angriffserkennung, die Aktivierung des Antispoofing (auf S. 42) und die Blockierung aller Protokolle mit Ausnahme von IP und ARP im Fenster **Einstellungen** im Bereich **Traffic-Steuerung** durchgeführt.

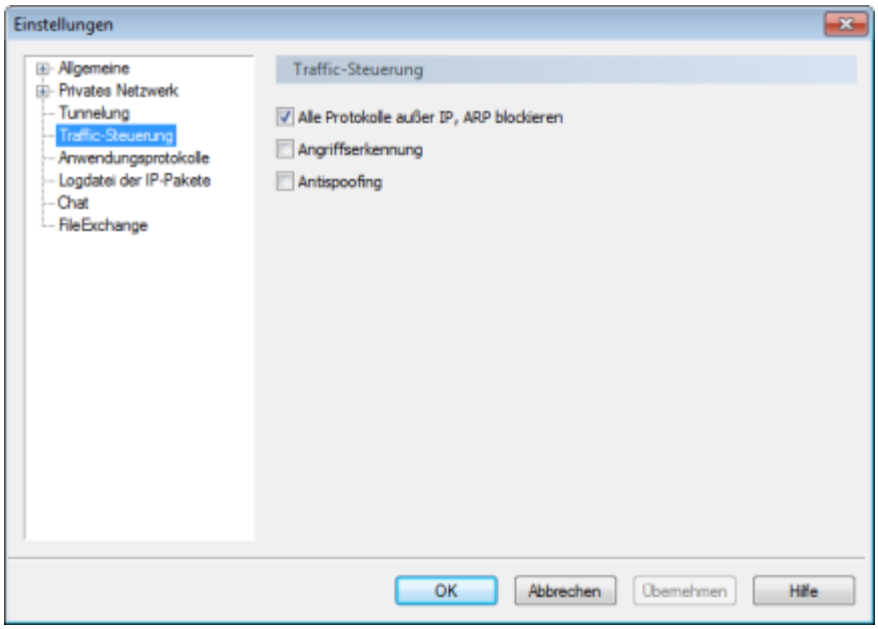

Abbildung 58. Steuerung des Traffics

In Version 4.x kann beim Starten von Windows eine Bildschirmtastatur für die Authentifizierung im Programm ViPNet Monitor verwendet werden. Klicken Sie dazu auf die Schaltfläche und wählen Sie im Menü den Eintrag **Bildschirmtastatur**.

Änderungen der Terminologie

Die Änderungen in der Terminologie, die in den Programmen ViPNet Client Monitor und ViPNet Coordinator Monitor der Version 4.x vorgenommen wurden, sind in der unteren Tabelle aufgelistet.

Tabelle 5. Änderungen in Benutzeroberfläche und Terminologie

Fachausdruck in Version 3.2.x	Fachausdruck in Version 4.x
Traffic-Filterregeln	Netzwerkfiltern
Export der Einstellungen	Einstellungen speichern

Fachausdruck in Version 3.2.x	Fachausdruck in Version 4.x
Import der Einstellungen	Einstellungen wiederherstellen
Sicherheitsrichtlinie (im Programm ViPNet Programmkontrolle)	Regeln der Programmkontrolle